Federal Ministry
of the Interior

Protection of Critical Infrastructures – Baseline Protection Concept

Recommendation for Companies

www.bmi.bund.de

Foreword

Infrastructures serve as vital lifelines in our societies. We are reliant on the supply of energy and water, information technology and mobility functioning in a dependable manner. Large-scale failures of these systems or other important infrastructures, even for only short periods, can have serious consequences.

The attacks in New York and Washington on 11 September 2001, in Madrid on 11 March 2004 and in London on 7 and 21 July 2005 demonstrated the dangers to which open societies are exposed. Combating international terrorism and protecting the population from such threats requires particular vigilance on the part of the security authorities.

Apart from averting terrorist attacks, other dangers also require to be addressed. Natural disasters such as floods, for example, can wreak substantial destruction.

Protecting so-called critical infrastructures - that is, facilities and organisations of major importance to the community whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences - requires a comprehensive approach. It is thus appropriate for the state and the business community to step up the dialogue on this topic and to develop joint solutions for enhanced security.

To this end, the Federal Ministry of the Interior, the Federal Office for Civil Protection and Disaster Response and the Federal Criminal Police Office have evolved a baseline protection concept. Expertise has been forthcoming from the business community to support this project from the very outset.

The Federal Ministry of the Interior would like to thank the security officers from
Deutsche Bahn AG, Mr Jens Puls,
Deutsche Flugsicherung GmbH, Mr Hans-Jürgen Morscheck,
Deutz AG, Mr Werner Becker,
IBM Deutschland GmbH, Mr Klaus Hintz,
Vattenfall Europe AG (Transmission), Mr Thomas Schäfer
and their staff for this support.

The baseline protection concept provides companies in Germany with recommendations from the point of view of internal security. The high security of infrastructures in Germany is an outstanding quality asset to the country. It is in the fundamental interest of the country's enterprises and citizens to safeguard this standard of security in the long term.

Contents

Summary 5

1 Aim and methodological basis 8

2 Hazards and endangered areas 14

2.1 Hazards 14

2.1.1 Hazards through natural events

2.1.2 Hazards through human and technical failure

2.1.3 Hazards through terrorism and criminal acts

2.2 Endangered areas in companies 23

2.2.1 Areas especially endangered through natural events

2.2.2 Areas especially endangered through human and technical failure

2.2.3 Areas especially endangered through terrorism and criminal acts

3 Generalizing recommendations for baseline protection 28

3.1 Analysis of protection requirements 28

3.1.1 Procedure for analysing protection requirements

3.1.2 Consideration of dependencies and interaction

3.1.3 Special consideration of terrorism and criminal acts

3.2 Definition of protection aims 33

3.3 Measures to achieve the protection aims **35**
3.3.1 Internal and external protection
3.3.2 Staff
3.3.3 Organisation and management

3.4 Risk management **39**
3.4.1 Emergency planning
3.4.2 Risk and crisis communication
3.4.3 Planning for the event of failures and Business Continuity Management

3.5 Quality management and documentation of protection measures **44**
3.5.1 Quality management of protection measures
3.5.2 Documentation of protection measures

4 Authorities/Institutions to be contacted **50**

Appendix 1: Questionnaire and checklist sample **53**

Appendix 2: Police information **75**

Appendix 3: Information of the Federal Office for Civil Protection and Disaster Response (BBK): “Für den Notfall vorgesorgt” (Excerpt in German on “Provision for emergencies”) **77**

Appendix 4: Glossary on baseline protection concept **97**

Appendix 5: For further reading (literature, Internet links) **102**

Summary

The aim of this baseline protection concept is to **reduce the vulnerability of critical infrastructures** to natural events and accidents as well as terrorist attacks and criminal acts. In this context it focuses on building-related, organisational, personal and technical protection measures.

Business background to risk management

The need for a baseline protection concept arises from statutory regulations and generally recognised standards,[1] as well as generally recognised business principles of anticipatory risk management and strategic business planning geared to success and continuity – in the form of so-called business continuity management (BCM), for example.

Target group: Company management

The initial target group for the development of **strategic concepts** for danger analysis, risk management systems and risk minimisation measures is top level management at infrastructure operators, who should bear the business risk and, where appropriate, liability risks in case of contraventions. The security officers are generally the points of contact at the companies for **implementation** of these strategic concepts. Implementation of the baseline protection concept is ultimately a task for the entire business in question, requiring support from all levels.

Trusting **co-operation between the state and infrastructure operators** is a prerequisite for clearly defining comprehensive protection measures. It is the operators who possess an adequate detailed knowledge of their infrastructures and are in a position to implement concrete protection measures in an effective manner. Agreement thus

[1] For example, Section 91 of the German Stock Corporation Act (establishment of risk management and monitoring systems), the Ordinance on Major Incidents, other general and specific obligations for operators and the new Basle II accord on capital standards.

first of all requires to be reached as to what **level of protection** is desired and acceptable.

Analysis/ planning process

The starting point is a multi-stage analysis and planning process covering identification of the given risks and a subsequent review, together with the adaptation of protective measures, where necessary. This process can be structured as follows:

The establishment of danger categories, differentiated according to the areas of natural disasters, accident, terrorism/crime,

based on the above, definition of the respective protection levels,

the development of damage and threat scenarios,

the analysis of weak points,

the formulation of protection objectives as a basis for the definition of protection measures and counter-measures,

definition of the required scope of action (coordination between public- and private-sector measures),

implementation of the defined required scope of action and

regular reviews of this analysis and planning process for the purposes of quality management.

Potential dangers for critical infrastructures are outlined as initial points of reference. These essentially cover dangers resulting from natural events, technical failure or human error and terrorism/criminal acts. On the basis of these defined dangers, particularly endangered areas at companies can be identified and generalised baseline protection recommendations can be drawn up.

Where this process is considered to be too cost-intensive or difficult to implement, such as at **small and medium-sized enterprises (SME)**, it may well be expedient to approach the matter in small steps, initially addressing aspects of the baseline protection concept that are considered especially urgent.

Questionaire / Checklist

A questionnaire and a checklist (Appendix 1), have been developed as an aid to operators of infrastructure facilities in implementing the baseline protection concept. The questionnaire and the checklist are designed as interdisciplinary instruments and are intended primarily to initiate a **discussion process within companies** on how to enhance and effectively control security. Both the questionnaire and the checklist are to be considered only as samples, rather than definitive inventories. This means that missing items require to be added in the course of the process and any inappropriate questions are to be modified or deleted accordingly.

The aim of this development process is to jointly set priorities from the perspective of internal security in close consultation with the infrastructure operators and to operationalise measures for the protection of critical infrastructures.

Contacts for the baseline protection concept:

Federal Office for Civil Protection and Disaster Response
Centre for the Protection of Critical Infrastructures
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Zentrum Schutz Kritischer Infrastrukturen
Deutschherrenstraße 93-95
53177 Bonn
BBK-Zentrum-I@bbk.bund.de

http://www.bbk.bund.de

Federal Criminal Police Office
Bundeskriminalamt
65173 Wiesbaden

http://www.bka.de or http://www.bundeskriminalamt.de

1.

Aim and methodological basis

KRITIS definition

In the face of the potential dangers posed by natural disasters, events resulting from technical failure or human error, terrorism or criminal acts, measures to ensure the fundamental security of our highly complex economic and social infrastructures appear crucial – particularly with regard to infrastructures "of **major importance** to the community whose failure or impairment would cause a **sustained shortage of supplies**, **significant disruptions** to public order or other **dramatic consequences**".[2] In addition to damage limitation and damage control measures, these so-called critical infrastructures necessitate first and foremost the development and availability of **preventive measures**, with the aid of which serious disruptions can be avoided from the outset or their consequences at least minimised.

Basis: Cooperation between state / business sector

Trusting cooperation between the state and operators of infrastructure facilities is essential to identifying and specifying necessary protection measures: While the state remains the guarantor for internal security and coordinates information and communication processes, only the operators, with their sufficiently detailed knowledge of their infrastructures, are in a position to implement concrete protective measures in an effective manner.

[2] Definition of critical infrastructures by the KRITIS task force at the Federal Ministry of the Interior on 17 November 2003

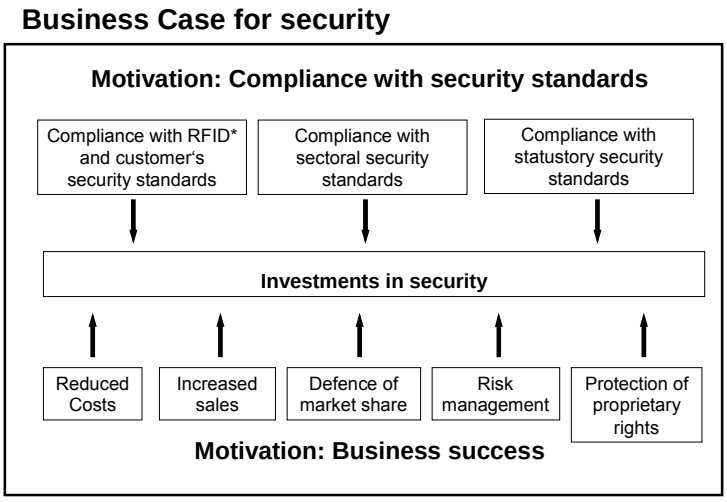
Starting points for a baseline protection concept are to be found in **statutory regulations** and in generally recognised **business principles** of anticipatory risk management and strategic business planning geared to success and continuity (in the form of so-called business continuity management (BCM), for example).

Risk management, operators' duties, relevant laws

Section 91 (2) of the German Stock Corporation Act (AktG), for example, obliges the board of management at a number of operating companies to undertake appropriate measures and to set up monitoring systems - such as a risk management system - in order to identify at an early juncture developments which threaten the continued existence of the company. Such developments include risk-entailing transactions and breaches of statutory regulations as well as dangers posed by natural events or acts of terror which may seriously affect the continued existence of the enterprise. Questions relating to the appraisal and assessment of business risks have acquired great emphasis not least of all as a result of the "Basle II" capital accord and the standards which have been adopted on money lending.

A further point of reference for measures to protect critical infrastructures lies in the operators' responsibility to safeguard their facilities against potential hazards and to undertake the necessary precautions. These **operators' duties** are regulated in part by statutory legislation (general operators' duties and specific duties pertaining to the Telecommunications Act or the Ordinance on Hazardous Substances for example, or to businesses which come under the ambit of the Ordinance on Major Incidents). Other duties on the part of operators stem from generally recognised business principles, such as the **principles of proper business management and business practice**. Other relevant regulations here include general and sectoral legislation, such as fire protection and fire prevention laws, building and planning law and environmental law or the law pertaining to the energy industry.

Figure 1: Motivation for security at companies



* Technologies such as RFID (Radio Frequency Identification), sensors, intelligent containers and software solutions for reporting and supply chain management can be combined with optimised processes and procedures to render the supply chain substantially more transparent.

Diagram and notes based on: Deloitte, Erfolg in der Secure Economy – Wachstum und Wohlstand in einer sicheren Wirtschaft. Executive Summary, 2004, p. 4 f.

Measures to prevent unauthorised interference

From the point of view of security, measures to prevent **interference by unauthorised persons** constitute a particularly important means of protecting critical infrastructures. Facilities are to be protected from disruptions resulting from criminal intent, natural events or accidents in such a manner as to eliminate as far as possible any serious danger, e.g. as a result of an explosion or the dispersion of hazardous substances. Failure of the provided products/services must also be avoided, in so far as such failure might give rise to substantial dangers in accordance with the above-stated KRITIS definition.

Aim: Reduction of vulnerability

The overriding concern of the baseline protection concept is to protect human life by **reducing the vulnerability of critical infrastructures** to natural events, incidents resulting from technical failure or human error and to terrorist attacks or criminal acts. The baseline protection concept is to incorporate structural, organisational, personal and technical standard safety measures.

What is **not** covered by the baseline protection concept

Notwithstanding the fact that environmental hazards can also constitute a serious threat, in the interests of a pragmatic approach this concept does not specifically cover **consequences limited to impact on the environment**. The same approach can be applied accordingly with regard to such consequences, however. Criminal attacks on companies which first and foremost damage the latters' competitive capacity, such as **industrial espionage**, are also excluded from the purview of this concept.

Finally, the **off-premises transportation of hazardous goods** is also excluded from the scope of the points discussed below. In principle, however, similar security considerations apply to the transportation of hazardous goods as are presented here for stationary facilities. Entrance and exit routes and, in particular, security for these routes must be examined in each individual case with regard to interfaces with the transport system and dealt with accordingly. The theft and/or intentional misuse of hazardous substances also require special consideration.

Attacks via companies' electronic networks ("cyber attacks") are also of importance. However, as the focus of this baseline protection concept is on averting physical dangers, with regard to **IT security** reference is made to existing concepts such as ISO standard 17799, the **IT Baseline Protection Manual** and the further recommendations from the Federal Office for Information Security (BSI).

Analysis/ planning process

In order to define workable and feasible measures, fundamental agreement requires to be achieved as to **what level of protection** is desired and acceptable. The following systematic approach is thus expedient for the purpose of evolving the protection concept:

I. The establishment of danger categories, differentiated according to the areas of natural disasters, incidents resulting from technical failure or human error, terrorism or criminal acts,

II. based on the above, definition of the respective protection levels,

III. the development of damage and threat scenarios,

IV. the analysis of weak points,

V. the formulation of protection objectives as a basis for the definition of protection measures and counter-measures,

VI. definition of the required scope of action (coordination between public and private-sector measures),

VII. implementation of the defined required scope of action and

VIII. regular reviews of this analysis and planning process for the purposes of quality management.

The competence and responsibility for implementing measures to realise the baseline protection concept lies with the operators. Aspects to be analysed in this context include:[3]

– **General risk assessment** (general safety situation, size and composition of the workforce, quality of the security organisation, social positions of members of the company management, nature of distribution links and activities abroad, criminality established to date, etc.)

– **Geographic location** of the operational area and the facilities (vulnerability from outside and within, distance from factory fence, visibility from outside, internal and external traffic routing, proximity to industrial areas or critical infrastructures, geological [e.g. risk or earthquakes] and geographic [e.g. proximity to rivers, topography] aspects)

– **Importance of the facilities** to up- and down-stream production processes and services (e.g. economic damage, production and delivery shortfalls)

– **Symbolic character** of the enterprise and/or facilities (type of production and storage of materials, product range, economic/strategic importance of the company)

[3] Modified acc. to the Hazard Commission, Maßnahmen gegen Eingriffe Unbefugter, *(measures to prevent unauthorised interference),* 2002.

– **Interdependencies**, i.e. interaction with other infrastructures

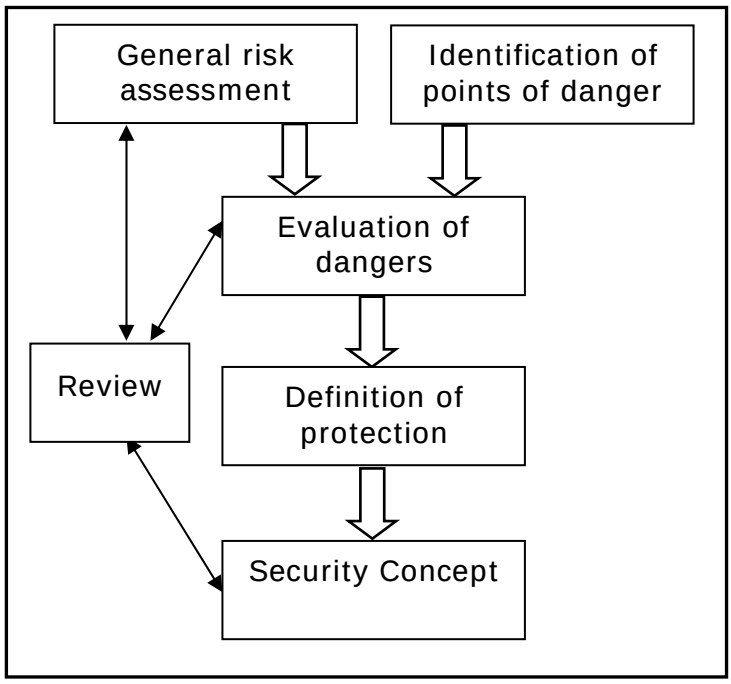
– Type, typology and cooperative relationships of the **risk management structures** implemented by the operator

– Structural nature of the **cooperation** between public facilities and operators, both with regard to emergency planning and crisis management and in terms of technical prevention.

–

In analysing these aspects, **secondary effects** are to be considered, as well as primary damage resulting from incidents (cf. p. 31).

Figure 2: Analysis steps



Source: Störfallkommission (German Hazard Commission), Maßnahmen gegen Eingriffe Unbefugter, 2002, p. 20

2.

Hazards and endangered areas

2.1 Hazards

Domino effects / delay / diversion

The hazards facing operators of critical infrastructures can be broken down into (2.1.1) hazards relating to natural events, (2.1.2) hazards relating to human error or technical failure and (2.1.3) hazards relating to terrorism or criminal acts. In this connection it is to be noted that an entire facility or security-critical parts of a facility may also be affected by events **outside of the actual facility**, in neighbouring operational areas or traffic facilities to which a special threat potential applies (**domino effect**). Possible impacts in this respect include the spread of fire from neighbouring facilities, flying debris after an explosion in neighbouring facilities, the failure of supplies after catastrophic events outside of the facility, etc. Events **occurring within a short time of each other**, such as a second, delayed explosion or several **incidents occurring around the same time** at different locations, may also entail an exponential effect by preventing rescue or restoration measures or causing resources to be concentrated in the wrong place, for example (**diversionary measures**).

Figure 3: Risk factors

Risk factors

The following overview is intended to illustrate the complexity and heterogeneity of the risk factors which require to be considered. It does not purport to be an exhaustive synopsis:

Risk factor: People

- *Inadequate security consciousness*
- *Inadequately qualified personnel*
- *Human error*
- *Criminal behaviour (sabotage, terrorist attacks)*

Risk factor: Organisation

- *Concentration of vital resources*
- *Outsourcing of infrastructures which are critical to the company*

Risk factor: Nature/environment

- *Natural disasters*
- *Epidemics*

Risk factor: IT

- *Complexity of systems*
- *Increasing IT-dependency*
- *Extensive, worldwide networking of IT systems*
- *Short IT innovation cycles*
- *Standardisation of technology and components*
- *Networking/interdependencies of critical infrastructures*
- *Internet as nerve system of critical infrastructures (connection to IT security)*

Source: Bundesverband deutscher Banken (Federal association of German banks), Management von Kritischen Infrastrukturen, 2004, p. 13

2.1.1 Hazards through natural events

Extreme weather situations

According to information from the insurance industry, a large proportion of elementary damage in Germany results from extreme atmospheric events. These include events such as high water (incl. rising of the groundwater level), flooding, storm tides, snow, ice, droughts and storms. Particular hazards apply during **flooding** as a result of the massive erosive impact of water on roads, bridges, dams etc. and from flotsam. The danger of drinking water contamination and attendant substantial health risks is increased by leaking harmful substances and refuse which are carried off in the floods. Rising groundwater levels may also cause flooding in more distant areas.

Hurricanes and hail may result from heavy thunderstorms and give rise to additional dangers. Air movements at a velocity of 75 km/h and over are defined as **storms**, while air movements of 120 km/h and over qualify as **hurricanes**. In addition to direct damage caused by wind pressure and subsequent gusts, storms and hurricanes can give rise to additional hazards resulting from debris and dirt which are entrained by the violently rotating funnel of a hurricane. Storms play a predominant role in terms of both frequency and the percentage share of damage caused to the economy.

In isolated cases, **hailstones** can measure over 10 cm and weigh more than a kilogram. Apart from causing damage to property and crops, hailstones can also inflict serious injury. Hailstones can also block water run-offs, resulting in flooding.

Earthquakes

The level of danger resulting from earthquakes inevitably rises according to the intensity of the earthquake. Depending on geological parameters such as soil characteristics, however, weaker earthquakes can also cause extensive damage to buildings and infrastructures. Secondary damage such as fires and tidal waves may also require consideration.

Key regions subject to a risk of earthquakes in Germany include the Kölner Bucht area to the west of Cologne, the Rhinegraben (Rhine rift system) and the Vogtland area.

Conflagrations

Conflagrations can be caused naturally by lightning, by spontaneous combustion or by wilful or negligent arson in combination with prolonged dry periods. The primary threat is to wooded areas, agricultural land and heathland.

Mass movements

Mass movements are caused by geophysical events (e.g. earthquakes, weathering), meteorological influences (e.g. heavy precipitation, flooding, snow and ice melts) and by anthropogenic influences (e.g. building measures, shock, deforestation). Examples of mass movements are avalanches, mudflows, hillside landslides and liquefaction of the soil.

Apart from direct damage, mass movements can also give rise to indirect hazards, by creating tidal waves in lakes or reservoirs or damming up rivers which subsequently burst free.

Epidemics

The term ‘epidemic’ refers to the occurrence of an infectious disease among humans or animals at high incidence within a short period of time over a broad geographic area. An increased risk of epidemics results from the global movement of goods, global tourism, intensive livestock farming, floods and droughts, for example.

A **pandemic** is an epidemic which spreads throughout several countries or even worldwide.

2.1.2 Hazards through human and technical failure

Fires

A fire may spread out of control as a result of human error, technical failure, arson (see 2.1.3 below), lightning, the release of hazardous substances or following explosions. Fires are classified according to their size as small-scale, medium-scale (e.g. fires in buildings) and large-scale fires (e.g. fires at industrial enterprises, large-scale plants, warehouses).

Release of hazardous substances

Hazardous substances include all substances of an atomic, biological, chemical or radiological nature (ABCR/CBRN) which can have a harmful effect on the environment or humans and/or may lead to explosions and fires. The properties of hazardous substances vary greatly, ranging from irritating through highly inflammable to explosive, environmentally hazardous, chronically harmful and toxic. The hazardous substances used at a company can be identified by means of an individual register of hazardous substances.

Explosions

An explosion is caused by a sudden expansion in the volume of gases due to the release of energy, leading to a blast wave and possibly also involving the generation of heat. Explosions result from human error, technical failure, wilful acts, lightning or the release of hazardous substances.

Other physical impacts from inside and outside

Physical impacts from inside and outside can be caused by accidents such as traffic or industrial accidents and plane crashes (cf. 2.1.3). Apart from destroying facilities, accidents can also lead to fires and explosions, to the release of hazardous substances and to other forms of damage.

2.1.3 Hazards through terrorism and criminal acts

Risk categories

Hazards relating to terrorism or criminal acts which are identified in the analysis of a company's general risk situation can be assigned to specific **graduated risk categories**. The respective levels here provide an overview of potential perpetrators, their possible or typical practices, their aims and motives and their degree of criminal energy. These risk levels enable a clear overview of which risks require to be considered.

While the assumptions within a risk category are based on empirical criminological knowledge, they must not apply precisely to every single case. Obviously, the question as to possible perpetrators and their mode of action cannot be answered with complete certainty. On the basis of experience acquired in safeguarding plants and facilities, however, it is possible to carry out rough classification in a table defining the given levels of risk according to **perpetrator groups**, their typical **motives** and possible **modes of behaviour** (cf. p. 47). Acts of negligence are not included in this assessment, as they fall under hazards relating to human error and technical failure (section 2.1.2.).

The extent to which potential perpetrators are actually able to cause serious damage and where such damage is possible and probable must be examined in the course of **risk assessment**, taking into account the points of danger identified in the company's environment (cf. "Risk management" section of the checklist, Appendix 1). The risk categories contain a number of assumptions which are intended to enable allocation to the determined threat level. These assumptions primarily concern

- possible background circumstances relating to the offence
- possible motives and typical modes of action
- resources which are likely to be employed
- the level of criminal energy to be expected.

Interference options can also be identified as a means of differentiation, establishing a link between perpetrators, their motivations and the options for action offered by the nature of the infrastructures concerned. The following **interference options** are conceivable in principle, for example:

Interference options

Deliberate maloperation

This option covers all intentional actions whereby a malfunction could be triggered by simple means, without the use of any tools or resources. Such actions could include, for example: switching facilities on/off, opening/closing closures in piping systems (valves/gates), turning handwheels and actuating levers in the course of a process. Deliberate maloperation can be carried out by a company's own personnel or by persons from outside the company.

Manipulation

Manipulation involves deliberately altering or adjusting parts of a system with the aim of inducing a critical status in the plant concerned. Possible examples here include programming control systems incorrectly, maladjusting measuring facilities, suppressing process signals, fault signals or alarms or shutting down protective systems. Insiders with a precise knowledge of the facilities are the primary suspects here.

Vehicle accident

Hazardous substances could be released or important parts of facilities could be damaged or destroyed as a result of road or rail traffic accidents. Examples here include leaking drums resulting from fork-lift accidents, derailing of tank wagons, destruction of facilities by lorry impact.

Interference using simple tools

This category covers intentional interference, usually of a spontaneous nature, in important parts of facilities, using the tools and resources which are available at every plant. Examples here include smashing glass parts of a plant, clamping moving parts of a plant or adding prohibited

substances or materials to the process. Company employees are the primary suspects here.

Interference using heavy tools

The planned violent destruction of parts of a plant is assumed for the purposes of this interference option. Possible tools employed in such attacks include crowbars, electric drills, flame cutters, bolt cutters or sledgehammers. Examples of such attacks include breaking open doors and subsequently destroying facilities, smashing up measurement and control facilities and smashing open containers and piping systems, resulting in large-scale leakages. Instead of a specific attack, vandalism may also occur, e.g. out of anger following a failed break-in.

Arson using simple resources

Simple resources cover ignition with matches, lighters or cigarette ends. This interference option thus only applies when sufficient quantities of combustible, highly inflammable materials are available. Examples here include igniting combustible liquids from a process, setting fire to storage locations to release hazardous substances, setting fire to peripheral rooms or facilities with subsequent impacts on important plant components.

Arson using fire-promoting resources

This category concerns fire attacks carried out with the aid of quickly and intensively burning materials. Examples of such attacks include pouring out and igniting combustible fluids (e.g. petrol), throwing so-called “Molotov cocktails” (e.g. through windows) or installing professional incendiary compounds with timing or remote ignition devices. Such attacks can also be carried out from outside (throwing distance) and require a pronounced level of criminal energy.

Use of explosives

Home-made, commercial or military explosives could be used here. Possible forms of attack include setting off a home-made “fire-extinguisher bomb” inside sensitive parts of

a facility or, more probably, at the periphery of a building, blowing up containers and piping systems, blowing away load-bearing components to cause containers to collapse, destroying plant components. This type of attack generally involves a radical political background and is carried out by perpetrators from outside the company.

Bombardment

Forms of bombardment can range from the simple use of air guns or catapults (steel balls) to the use of heavy weapons - e.g. anti-aircraft missiles - by terrorist perpetrators. Possible methods of interference here include causing leaks in outdoor containers or in pipelines, inducing an explosion. Bombardment is possible above all from outside the outer fencing of an operational area or industrial estate, whereby facilities installed in the vicinity of the fence are at a greater risk.

Plane crash

Both the kinetic energy of crashing aircraft and the explosive impact of the fuel or any explosives on board require to be considered here. An aircraft can also be used as a means of transport to propagate ABCR substances. Attacks leading to plane crashes may take place from outside, e.g. by rocket attack, remote ignition of explosives, remote manipulation of the on-board electronics, failure/abuse of air traffic control centres, or from inside by taking over/interfering with the control system or by igniting explosives (suicide attackers).

Deployment of ABCR weapons

Depending on the availability of corresponding agents and resources, there is a broad range of conceivable possibilities requiring special discussion. Possible forms of deployment range from the intentional spreading of diseases (mailing of anthrax pathogens) or epidemics (introduction of highly infectious pathogens into supply systems or the air we breathe) through the use of so-called “dirty bombs” aimed at causing sustained public disquiet to the use of poison gas at traffic junctions, for example.

Combined effects

A broad spectrum of possibilities is conceivable here, too, from the above-mentioned dirty bombs as a combination of explosive impact and radioactive contamination through the destruction of a production plant combined with the propagation of harmful substances to individual publicity-grabbing actions with far-reaching consequences for corporate activities or public utilities.

2.2 Endangered areas in companies

Critical infrastructures, as well as individual production or service areas within a facility, are subject to different levels of risk from natural events, human error, technical failure, terrorism or criminal acts. At company level, additional risks can arise as a result of **job cutting,** the **centralisation** and **automation** of control and monitoring processes, shifts in areas of responsibility resulting from **outsourcing** or the inadequate implementation of required measures as a result of cost pressure.

2.2.1 Areas especially endangered through natural events

Areas at special risk from extreme weather conditions

Storm tides and flash floods can lead to the destruction of entire buildings and plants. Areas at particular risk include networks, buildings, production, extracting and processing plants and non-electronic data records. Slowly draining floods lead primarily to damage in lower-lying areas of buildings (basement, ground floor). As damage resulting from the effects of water generally leads to network failures, information and communication technology, the (internal) power supply, supply networks and other networks are at particular risk. Outside of flooded areas, such damage can be caused by rising groundwater levels.

All buildings and facilities are exposed to storms, irrespective of their location. At particular risk, however, are buildings and facilities in exposed locations (mountains, hills, mountain ridges, snow paths) and buildings and facilities whose design exposes them to storms.

Storms, as well as droughts or extreme frost, can also lead to supply shortages which threaten the continuation of normal operations.

Areas at special risk from earthquakes

Earthquakes can damage or destroy buildings and entire complexes and lead to failures and breakdowns in all areas. The risk of even minor tremors causing damage in the area of IT and in vibration-sensitive areas of production, extraction and processing cannot be ruled out.

Areas at special risk from conflagrations

Conflagrations can cause damage in all areas in which buildings or facilities are located. Conflagrations can additionally lead to entire areas or traffic routes being closed off, as a result of which facilities become difficult or impossible to access.

Areas at special risk from mass movements

Mass movements can damage or destroy buildings and facilities as a whole or block access to such buildings and facilities. Mass movements outside of a facility involving effects on external networks can also lead to supply shortages which threaten the continuation of normal operations.

Areas at special risk from epidemics

Epidemics can lead to unavailability or shortages with regard to the specialist personnel which is required to operate facilities. Production operations, computer centres and control centres would be particularly seriously affected by such circumstances. In addition, the closing-off of areas

during human and livestock epidemics may render it difficult or impossible to access facilities.

2.2.2 Areas especially endangered through human and technical failure

Areas at special risk from fires

Fires can act on facilities and buildings from within and from outside. They can destroy or damage all areas, or they may prevent further use due to the effects of smoke. Even small fires in exposed parts of facilities (e.g. IT) may lead to failure of the entire facility.

Areas at special risk from hazardous substances

In addition to the primary risks of harm to the operating personnel and damage to the area surrounding the facility concerned, the release of hazardous substances may also induce explosions and fires. The further use of contaminated technical facilities, including IT equipment, may be impossible or restricted.

Areas at special risk from explosions

Explosions can impact on facilities and buildings from within and from outside. They may damage or destroy all areas and induce chain reactions. The primary destruction results from the blast wave; the initial explosion is often followed by fires. Even small fires in sensitive areas (IT, power) may lead to failure of the entire facility.

Areas at special risk from other physical impacts from inside and outside

Physical impacts from inside and outside may impair the functional effectiveness of facilities or buildings and damage or destroy entire complexes. This can lead to breakdowns and failures in all areas. Physical impacts in the area of external networks can lead to internal supply shortages and production losses.

2.2.3 Areas especially endangered through terrorism and criminal acts

The graduated risk categories indicating conceivable threats initially apply to the entire company. However, individual complexes within the overall company are also comprised of units or plant components which differ in terms of risk potential, design, form of usage, technical configuration and, above all, vulnerability to interference and malfunctions.

Points of special vulnerability generally also exist within plant components. Where appropriate, these are to be ascertained by means of a separate systematic examination. By way of analogy to the security report which is to be drawn up in accordance with Section 9 of the Ordinance on Major Incidents (Störfallverordnung), both the actual risk potentials and the facilities operated to supply and control the facilities and the materials transport systems, etc. are also of importance with regard to installation protection.

Classification of security areas

Consequently, it is generally expedient to break down the operational area into a number of sub-areas of different types and risk categories. A complete analysis of all potential weak points combined with the diverse scope of conceivable forms of attack or impact would result in an unmanageable number of different variants. It would thus appear expedient to group together areas and parts of facilities in a more generalised manner. It may be useful, for example, to consider a continuous complex as a whole, without considering in greater detail which individual components and parts are vulnerable and what precise impact a potential attack on one or other of the facility's components might have. The complex concerned is then classified as security-critical and secured as a whole in such a manner as to cover all the individual components.

In the case of supply systems which are deployed throughout the operational area, sub-segments concerning threatened installations should ideally be established and the examination process should not be extended unnecessarily

to include comprehensive complete networks. At the same time, a **view** extending **beyond** the **company's perimeters** remains important, with regard to both special risks in the area of the up- and down-stream value chain and **geographic interactions** with neighbouring hazardous area.

Definition of sub-areas

It may be expedient to group together hazardous areas as follows, for example:

- Production, extraction and processing plants
- Control centres, IT systems
- (Unmanned) external facilities
- Service lines
- All kinds of power supply systems
- All kinds of emergency power units

3.

Generalising recommendations for baseline protection

Baseline protection defining minimum required level of proection

The aim is to present baseline protection requirements for different hazards, which are to be regarded as representing the minimum level of protection required for stationary facilities in the area of critical infrastructures. A **multi-stage process** based on the approach described in section 1 (Objectives and methodical basis, p. 11) is appropriate here, covering identification of the given risks and the development and implementation of various protection measures.

3.1 Analysis of protection requirements

3.1.1 Procedure for analysing protection requirements

Risk assessment

Firstly, the **locations** of the KRITIS facilities are to be examined. This includes risk assessment with regard to natural events, events resulting from technical failure and human error, and terrorist attacks and criminal acts. Risk assessments regarding dangers from natural events can be carried out on the basis of plans (flooding plans, earthquake maps, regional development plans, risk maps) which can be

obtained from the competent authorities (cf. section 4). With regard to dangers relating to human error and technical failure, due compliance with relevant rules and technical regulations (e.g. fire protection, Ordinance on Hazardous Substances, occupational health and safety, training) is to be verified. Regarding terrorist threats, operators of critical infrastructures can

- undertake systematic assessments of critical areas of the company and facilities in cooperation with the authorities which are responsible for internal security (cf. section 4) in order to establish whether they may constitute a key target in principle, in view of which the **possibility** of the impairment, interference with or destruction of the facility concerned exists (**danger analysis**)
- examine in cooperation with the authorities responsible for averting dangers outside of the company (cf. section 4) what concrete **consequences** are to be expected as a result of the possible impairment, interference with or destruction of the given facility, and whether these might lead to a **serious danger** (**hazard analysis**)
- assess contrasting and common requirements pertaining to protection from interference by unauthorised persons, from natural hazards and from human error and technical failure.

Agreement on level of protection

Danger analysis and hazard analysis are to be accorded equal priority in analysing protection requirements. It should be decided in each individual case which of these steps is to be undertaken first. For the purposes of this concept it is suggested to begin with a general danger analysis and then to determine the concrete consequences of these dangers for the company by means of a hazard analysis. The required level of protection can subsequently be discussed on the basis of this analysis process and duly defined.

The analysis and the resultant measures should be documented (cf. section 3.5.2). This **documentation** is of a particularly confidential nature, however, and should only be accessible to a limited group of employees even within the company. Documents which are available to the personnel as a whole and to the public should, however, verify that the

operator has undertaken the necessary measures to secure the relevant area of the company and the facilities (cf. section 3.3.1).

The analysis is furthermore to be **repeated** at regular intervals and/or integrated into the company's risk management process, in order to enable the identification of new dangers, to carry out any **reassessment** which may be necessary, to adapt the protection requirements accordingly and thus to ensure that the basic protection remains up to date.

3.1.2 Consideration of dependencies and interaction

In addition to direct dangers pertaining to natural events, human error and technical failure or terrorism and criminal acts, critical infrastructures are also exposed to indirect dangers. These require to be considered in carrying out a comprehensive analysis of protection requirements.

Domino effects

Firstly, the so-called **domino effects** are to be identified. These occur when external events, e.g. in neighbouring operational areas, in the surrounding area or in the traffic area, impact on the facility. By way of example, natural events occurring some distance away, such as floods, mass movements or earthquakes, can affect the functional effectiveness of the facility as a result of backwater or blocked access and delivery routes. Malfunctions in surrounding facilities, particularly such facilities as are subject to a special risk of danger, may damage the facility as a result of an encroaching fire or flying debris after an explosion. The failure of supply facilities such as energy and water supply systems or of services from suppliers is also possible as a result of catastrophic events outside of the facility.

Events **occurring within a short time of each other**, such as several incidents occurring around the same time at different locations or a **second, delayed explosion** may also

entail an exponential effect by preventing rescue or restoration measures or causing resources to be concentrated in the wrong place, for example (**diversionary measures**).

Secondary damage

Beyond this, additional damage (**secondary damage**) may result from the impairment of critical infrastructures, such as supply bottlenecks and shortages linked to disruptions to the transport system following a power failure. Such secondary damage is also to be considered in analysing the protection requirements, in order to enable an adequate assessment of the effects of the complete or localised failure of critical infrastructures on areas both within and outside of the facility.

3.1.3 Special consideration of terrorism and criminal acts

Previously drawn up danger and hazard analyses and security concepts should be examined to ascertain whether they also accord due consideration to such dangers which, according to the danger analysis, may result from **interference by unauthorised persons**, even if these dangers have been largely ruled out in the form of malfunctions, natural risks or accidents.

If the hazard analysis has established that a serious danger may exist for special objects of protection, it is to be examined to what extent the facilities may appear particularly “attractive” for terrorist attacks or criminal acts. To this end, a systematic analysis is to be carried out, focusing in particular on the following aspects which have already been mentioned in section 1 (Objectives and methodical basis, p. 11):

Contents of the analysis/ planning process

- General **risk assessment**
- **Geographic location** of the operational area and the facilities
- **Importance of the facilities** to up- and down-stream production processes and services

- **Symbolic character** of the enterprise and/or facilities
- **Interdependencies**, i.e. interaction with other infrastructures
- Type, typology and cooperative relationships of the **risk management structures** implemented by the operator
- Structural nature of the **cooperation** between public facilities and operators.

Cooperation with security authorities

Operators will be required to obtain some of the information necessary for this purpose from the authorities responsible for internal security (cf. section 4). The involvement of these authorities is generally recommendable at this stage.

The **general security situation** describes dangers such as generally apply to operational areas, where appropriate with regional differences. An initial **indicator** of relevant criminality is provided by police crime statistics and publications by insurance agencies. The security situation with regard to politically motivated offences is defined by ongoing appraisals by the authorities on the basis of their operations relating to judicial police activities and the protection of the constitution. **Regional aspects** can also be allocated a stronger focus on the basis of this information.

The scope, severity and nature of **previously recorded offences** in an operational area can provide an indication of the level of danger. A period of around **five years** can be reviewed for this purpose. The following information should be contained in such a review:

- General information on recorded minor offences, such as simple theft
- Number of previously committed break-ins or serious cases of theft
- Identification of organised criminality in the operational area
- Number of previously perpetrated acts of sabotage, including unresolved cases involving a substantial suspicion of sabotage

- Number of previous bomb threats or other threatening acts
- Number of previous arson attacks or attacks with explosives, including suspected cases.

3.2 Definition of protection aim

To enable the stipulation and operationalisation of protection objectives and to establish such objectives as an inherent part of corporate policy, it is recommendable to define them as part of a security management system. In the past, management systems have proven an effective instrument for the systematic handling and examination of corporate processes and procedures, as long as they were able to ensure a successful synthesis of top-down approaches (hierarchic, centralised), bottom-up approaches (discursive, decentralised) and an open-minded approach (innovative, networked). The **systematic integration of various security-relevant processes**, including both mutual integration and integration with value creation strategies, is particularly crucial in the context of **corporate security**. Many of these measures are already in use or can be introduced comparatively quickly. If they have not already done so, operators should appraise the effectiveness of existing measures and take any necessary action on the basis of their findings (cf. section 3.5.1).

The quality and extent of personnel and technical resources for the company's internal and/or external **security service** (e.g. plant security) are of particular importance in this context; appurtenant requirements are defined in DIN 77200, for example. Particular emphasis is also to be attached to **networking** and **harmonising elements of security management** which are often largely autonomous, such as IT security, installation protection and personnel security. When the operational area under review belongs to a larger enterprise (corporate division, subsidiary, majority-owned company, etc.), the level of threat and danger facing the enterprise as a whole must additionally be considered. This

applies above all with regard to politically motivated crimes. Past experience shows that this danger generally increases according to the size and (global) significance of the enterprise as a whole.

In this connection it should also be established whether **increased risks** apply as a result of certain **distribution links**. This could be the case if business links exist with politically instable countries, for example. As export-oriented operational areas generally supply goods all over the world, an increased risk applies above all when particularly prominent links exist with such countries.

Key protection objectives

Key protection objectives to secure facilities and installations which are assessed as being security-critical can be described as follows:

- The boundaries of operational areas are to be secured by technical and organisational measures such that unauthorised persons are unable to enter into these areas without the use of force or malicious deceit and such as to ensure that any forced entry will be detected within a reasonable time.
- Outsiders should be identifiable.
- The facilities themselves are to be secured such that no unauthorised interference can be carried out without internal knowledge and/or technical resources.
- Financial resources should be deployed according to lists of priorities (**integrated security management**).
- **Industrial estates** impose special requirements with regard to security measures on account of the large number of legally and organisationally independent operators alone. As a rule, the vulnerability of dangerous facilities can only be minimised through jointly defined protection objectives and measures. Suitable measures are most expediently selected by means of a systematic security analysis.

3.3 Measures to achieve the protection aims

Measures to prevent unauthorised interference

Objectives should be **defined** for the protection of facilities and installations which are assessed as being security-critical. For many years now, operators of facilities subject to the Störfallverordnung Ordinance on Major Incidents have been obliged to secure their operational areas and facilities in order to prevent unauthorised interference, for example. In view of specific threat situations (terrorism), it is **also** necessary to hinder the entry of unauthorised persons into **operational facilities of critical infrastructures which are not directly subject to the Ordinance on Major Incidents**. Effective measures here include monitored fencing, the organisation of gate checks, patrols, video surveillance, etc. (cf. checklist, Appendix 1).

The risk of terrorist attacks on operational areas/facilities is to be considered with due regard to the probability of such attacks on the one hand and the potential consequences on the other. **Security measures** which have been **commonly employed** to date continue to offer **substantial protection**. Such measures should thus be applied systematically and with due consideration of the recommendations provided in this concept, insofar as they appear necessary in the wake of 9/11/2001 and have yet to be implemented. Facilities and/or parts of facilities which are particularly dangerous and at risk of terrorist attacks are to be provided with additional security measures.

In order to achieve the defined protection objectives, appropriate measures are to be undertaken. These can be broken down into internal and external protection measures (physical protection), personnel protection measures, organisational protection measures and management measures.

3.3.1 Internal and external protection

The measures to achieve the security objectives for the internal and external protection of facilities include the following, for example:

- Particularly sensitive areas should **not** be built in **regions which are subject to a risk of flooding and earthquakes.** If they are already located in such regions, relocation to non-endangered regions should be considered; as a minimum precaution, special measures should be undertaken to afford protection from flooding and earthquakes (e.g. raising of IT facilities and power distribution installations, cushioning against vibration, diking).

Making facilities robust and controlling access

- All facilities and particularly sensitive parts of facilities should be made more robust, in order to reduce or avoid consequences of storm tides, flash floods, earthquakes, of physical forces and of explosions. Adequate reserve resistance capacities are to be incorporated into the lower storeys (pressure compensation). Particularly **sensitive areas** should furthermore be located **inside the facilities**.
- Locating facilities and installations requiring protection such that accessing them requires a certain **distance** to be covered and takes a certain **time** is a key aspect in preventing terrorist attacks and sabotage. Barriers and obstacles can hinder or prevent access to sensitive areas (access zones, access controls, plant security, gates, fencing, patrols, bollards, concrete elements, elevations).
- Concealed areas can be monitored with electronic security systems (video surveillance, motion detectors, noise sensors, thermal imaging cameras, night vision devices).
- The importance of gates to security generally extends beyond controlling access. In this context, the question as to **security for the gates** themselves arises. If, for example, the main gate is the sole point for receiving alarm and fault messages (frequently after the normal service hours of the operating area concerned), it must not be possible to prevent the relay of these messages to support centres by interfering with the communication facilities or threatening the security staff at the gate. This

is to be ensured via appropriate protection measures. It is also of central importance that the gate / security centre be continuously manned.

- An **understanding** of security considerations for the operating area is to be instilled in the **personnel**, who are also to be involved in security processes through team training, seminars, etc.

Basic protection – special protection

In most cases, the measures to secure the site as a whole serve to provide **basic protection**; they provide an initial barrier to ward off unauthorised persons. Special individual protection is additionally required for all points of danger. “Classical” measures to secure facilities and installations play a major role here.

Securing individual danger areas usually represents the most important preventive measure, as the “external” measures which apply to the entire operational area rarely afford complete and adequate protection.

External protection measures will not affect any risk of wilful action on the part of employees, for example. Similarly, 100 per cent control of access to the operational area or installations (e.g. at the beginning of shifts or at peak traffic times) is practically impossible. On the other hand, there is scope for substantially **more effective controls** at **individual points** of the operational area.

3.3.2 Staff

Attacks on a company can always be carried out by both external and **internal perpetrators.** While a considerable number of concepts are available for protection against attacks from outside, there is a pronounced need for action in the area of possible threats from internal perpetrators. This category of perpetrator concerns company employees or outsiders who legitimately gain access to the area of security-critical facilities, but who undertake unauthorised

actions. They may have a good knowledge of the facilities concerned and aim to use this knowledge to criminal ends.

Instilling a due awareness in the personnel

Both the state, as the guarantor of internal security, and the operators of infrastructure facilities are obliged to develop and apply preventive measures here. In addition to the general measures implemented by the security authorities, preventive measures are also required on the part of operators. These measures pertain above all to the area of **personnel management** and **personnel surveillance** (instilling a sense of identification with the company, motivation, sensitive handling of measures which impose a strain on personnel, training of superiors, etc.). Beyond this, a general appreciation of this problem area should be instilled in the entire workforce. Advice from qualified specialists in this field may be expedient. Use should also be made of carrying out a **security check** on employees in highly sensitive areas. For the purposes of an initial analysis, information should be available on the number of leased workers or employees from outside companies present within the company, their connection to the operational area (in particular the length of their involvement) and the average number of visitors. Further advice and information on preventive measures in the area of personnel is available from the competent authorities, in particular police stations, the Land criminal police offices, the Federal Criminal Police Office and the Land and Federal offices for the protection of the constitution.

3.3.3 Organisation and management

The internal organisational set-up, in particular measures relating to the **structuring of operations**, and the management system form an important framework into which various individual measures require to be incorporated and checked on a regular basis in order to ensure effective functioning of the overall security system. The following aspects should be addressed in this context:

Structuring of operations

- The corporate identity card system, covering the issuance/return of I.D. cards, I.D. card encoding (type and procedures), storage of I.D. cards (measures to prevent unauthorised access), areas of authority (to be defined along the same lines for passwords and electronic access rights)
- The procedures for appointing and monitoring personnel performing security-related duties, access permits for areas/workplaces which are potentially at risk
- Personnel training and instruction, e.g. to prevent maloperation
- Rules pertaining to supervision and regular checks on work in security-critical areas
- Details of the keys system, covering the locking system (type, scope, age), issuance, return and registration of keys and storage of keys and cylinders
- Cleaning in security-critical areas by internal or external personnel, cleaning times, supervision of cleaning, personnel monitoring (for external personnel)
- Listing of standing instructions for all measures relating to security
- Alarm plans for fires/explosions, leakages, environmental hazards, plant-specific events, hostage-taking, extortion, etc.
- Regular revision and updating of the baseline protection concept, in particular the protection requirements, the protection objectives and the catalogue of measures.

3.4 Risk management

Risk management cycle

To date, risk management systems as a means of enhancing a company's security have always been set up on a voluntary basis. Following the amendment of the German Stock Corporation Act (Section 91 (2)), certain companies are now **obliged** to set up a monitoring system in order to identify in good time "developments threatening the continued existence of the company". The basis for risk

management systems is provided by the definition of a risks policy as part of the corporate business policy, stipulating guidelines for dealing with risks. Risk management systems are generally developed according to the multi-phase model comprising risk analysis, risk control/handling, risk monitoring and risk financing, on the basis of the risks policy adopted for the company:

- In the risk analysis process, **all risks** of **relevance** to the company, including the dangers described in the baseline protection concept, are to be identified, analysed and evaluated on an individual basis for each company.
- Risk control serves to **avoid** or minimise **risks** and to pass on risks to third parties (customers, insurance companies, etc.); a **residual risk** will have to be accepted.
- In the course of risk monitoring, **early warning and controlling systems** are to be set up and the corporate **risks policy** is to be adapted, if and as necessary
- Of major importance to companies is the question of risk financing, whereby the focus here must be on a **medium- to long-term assessment**, to enable an adequate appraisal of the benefits of investing in security, such as competitive advantages, for example.

In an institutional context, the introduction of risk management systems can be supported by appointing a **risks officer** to evolve a risk management system and adapt this system to changing underlying conditions on an ongoing basis in cooperation with the staff responsible for security matters within the company and competent (official and non-official) bodies outside of the company.

3.4.1 Emergency planning

In the event of impairment, interference with or destruction of an infrastructure facility, operators are to undertake measures to **minimise** the **consequences**. In order to control the consequences of a disruption or crisis on critical

infrastructures, information must be available to the hazard control authorities on the facilities and on undertaken and planned measures. In turn, these authorities must implement the scenarios in their own alarm and hazard control plans. The following recommendations apply with regard to measures to limit the consequences of the above-mentioned events:

Cooperation with hazard control authorities

- In their **own interest**, operators of facilities and installations which are not subject to extended statutory obligations such as the Störfallverordnung Ordinance on Major Incidents, but which have been established to be security-critical, should also contact the hazard control authorities forthwith and furnish the necessary information to enable the drafting of external alarm and hazard control plans. The immission control and hazard control authorities should consult one another for the purpose of identifying such potentially security-critical facilities.
- On the basis of the information available from the operators, the competent hazard control authorities should draw up the necessary **external alarm and hazard control plans** for the protection of the population forthwith.
- **Action plans** to be applied in case of disasters should be drawn up and revised on a regular basis (e.g. telephone lists, allocation of responsibilities, procedures). This area of work also includes preparations for effectively functioning **crisis communications**.
- A **reporting centre** should be set up. Personnel who will come together in the event of a crisis are to be appointed and kept available. Appropriate premises are also required. These should be secured against external influences and equipped with functioning communications facilities.

The drafting, implementation and regular review of **emergency concepts** to cope with the **unavailability of personnel** is also recommended.

3.4.2 Risk and crisis communication

Commensurate communication of the maximum possible efficiency is of pre-eminent importance both ahead of possible crisis events and, in particular, after the occurrence of serious damage relating to critical infrastructures. To this end a **communication concept** should be available, covering the following elements, for example:

Crisis communications

- Prior to the occurrence of a crisis, which can never be fully ruled out, **appropriate forms of communication** must be identified and promoted in order to inform and instil the necessary understanding in the population, should a crisis event occur.
- As complete protection can never be guaranteed, measures pertaining to **external hazard control** are of particular importance in the anticipatory phase. The competent authorities must receive the necessary information from the operators and undertake the measures which fall within their scope of authority. A substantial proportion of the information required to enable assessment of the threat situation by the operators and the authorities must be available on the basis of the regulations pertaining to the security report (Section 9 of Störfallverordnung) and to the alarm and hazard control plans (Section 10 of Störfallverordnung, Land laws on fire protection and disaster management). For facilities relating to critical infrastructures which are not subject to the Ordinance on Major Incidents, the necessary information should be gathered and documented as an essential element of **integrated security management**.

Coordination of communication channels

- Swift action and communications are of crucial importance in crises. In such situations, the public and private sectors need to respond in a coordinated and practical manner. Against this background, the appropriate forms of internal and external communications should be defined in advance, according special consideration to the electronic media (**and their possible failure**). It should be defined how communications are to be carried out via e-mail, websites, classic and mobile telephony and via radio, including a definition of central flows of information and reporting

channels. An analysis of the (global) media situation is also of special importance in this context, as in many cases the **psychological effect** can dramatise events which are actually of only limited severity.

- Particular attention is to be devoted to parts of the company (e.g. facilities) where, in the area of installations meriting special protection, there is a **threat to human life** or serious **harm to people's health** is to be feared. This information is crucial to efficient communications with government agencies and should also form an integral part of the corporate baseline protection concept.
- On the question of any concerns regarding the publication of sensitive data, the vested interests concerned require to be weighed up carefully in each individual case concerned. It is to be noted that **informing** third parties of risks pertaining to them not only constitutes a right of individual liberty but also serves as a **precautionary element**. In addition to weighing up vested interests, appropriate criteria thus require to be developed in order weigh up the possible loss of security against a possible gain in protection.

Risk communications: Publication of sensitive data

3.4.3 Planning for the event of failure and Business Continuity Management

Contingency planning

In order to enable business operations to be largely maintained in the event of a crisis, or at least to set up **emergency operations** and to restore full functionality as quickly as possible, concepts for contingency planning and business continuity measures must be defined in good time. As precautionary measures, contingency and restarting planning goes beyond direct emergency management to handle the current crisis; the drafting of these central instruments of crisis management requires to be **initiated** and **overseen** by the **top management**. In particular, contingency plans should incorporate alternative concepts for the organisation of central business processes in the event of the failure of critical areas at the company and among suppliers and service providers, as well as according due consideration to the provision of **redundant capacities** and

an alternative location. The planning is to cover the following points at least:

- Redundant systems should be provided for particularly sensitive areas (e.g. emergency power supply, data lines, multiple-line production). For security reasons, these should be located in **separate areas.**
- An adequate **level of operating supplies** is to be provided for operation of the facilities (e.g. for production, emergency power supply and other vital processes). Special consideration is to be given here to the effects of large-scale incidents extending over several days (e.g. impassable access routes, prolonged power failures).
- Aspects of the **fault-tolerant design** of equipment, facilities and processes should receive due consideration in the course of planning and operation (limitation of effects).
- As a precaution against the unavailability of personnel, e.g. as a result of epidemics, **adequate manpower** should be available, particularly in key posts. The drafting, implementation and regular review of emergency concepts to cope with the unavailability of personnel is recommended.
- Contingency and emergency plans are to be revised on a regular basis and adapted to new developments.

3.5 Quality management and documentation of protection measures

3.5.1 Quality management of protection measures

Integration into existing quality management system

In order to ensure that protection measures as proposed in the baseline protection concept, for example, are realised in accordance with the given requirements and **optimised** in an ongoing **improvement process**, the protection concepts should be subject to quality management. It is

recommendable to integrate the sub-concept “Quality management of protection measures” into an existing in-house quality management system and to define and document areas of responsibility. This will establish quality management in the area of the protection measures as an integral part of **corporate policy** which is assigned to the **top management’s** scope of duties.

To ensure successful implementation of the protection measures and ongoing review, the requirements must be specified in clear and concrete terms. The **s.m.a.r.t.** criteria offer a useful guideline here:

s (specific): What precisely is to be achieved and on what scale?

m (measurable): Are there measurement criteria/yardsticks, on the basis of which the degree to which the set objectives are achieved can be measured and monitored? Have checklists been drawn up accordingly?

a (attractive, accepted): Is the objective ambitious, can attainment of the objective be actively influenced with the available resources?

r (realistic, realisable): Is the objective attainable with due regard to the underlying circumstances and available resources?

t (timing): Has a deadline been set within which the objective (or interim goals) is to be achieved?

Quality management control cycle

Far from being a static process, quality management follows a control cycle comprising planning, implementation, analysis and adjustment, giving rise to a continuous improvement process. The protection measures are thus also to undergo regular monitoring and means of **adjustment** in case of non-conformance (e.g. follow-up training of security personnel, adaptation of processes, etc.) are to be implemented.

3.5.2 Documentation of protection measures

The protection measures for each individual point of danger are to be documented in a corporate baseline protection concept, whereby it may be expedient to group the measures together according to areas, buildings, sections or functional units. It goes without saying that this information is of a **particularly confidential** nature. The following aspects should be considered for individual points of danger:

- Location on the site (site plan), location within buildings or areas (ground plan)
- Points of access for persons and vehicles, escape routes
- Structural/mechanical design of partitions between areas (walls, fences)
- Structural design of buildings and security-critical rooms (materials, reinforcement, wall thicknesses)
- Mechanical securing of doors, windows and openings
- Electronic surveillance measures for doors, windows, rooms, etc.
- Access control procedures for the relevant points during and after normal operating hours for personnel and outsiders
- Measures to safeguard individual control elements against maloperation or sabotage, e.g. mechanical locks or electronic monitoring
- Installation of information and warning signs
- Special security measures
- Work and shift times of the department concerned, differentiation of security measures if appropriate
- Patrols of the facilities and installations by plant security force (patrol routes, patrol times).

Table of risk categories

	Risk category 1	Risk category 2	Risk category 3
Intention:	The perpetrator (offender) intends to cause damage on a limited scale. He is unaware of or willing to accept the risk of a far more dangerous situation. (Qualified intent).	The perpetrator (offender) intends to cause large-scale damage and an attendant general situation of danger, possibly as a diversionary tactic. (Direct intent).	The perpetrator (offender) intends to carry out massive attacks with a beacon effect. (Brutal mode of behaviour constituting a public danger)
Motivation:	Revenge, frustration, to "demonstrate" shortcomings, to achieve political effects, to attract attention, to extort protection money	(Homegrown) political radicalism, attainment of substantial pecuniary / competitive advantages	Anarchism, bringing about social change by violence, "punishing" companies (also in a representative capacity for states) or governments, religious motives
Preparatory acts:	Spying, procurement of tools and other resources.	Reconnoitring security-critical parts of facilities and weak points; possibly specifically exploiting gaps in surveillance. Procurement of special resources; possibly deactivating security devices.	Logistical preparations, spying, deactivation of security systems.
Resources:	Simple and heavy tools; possibly simple incendiary devices.	Simple and special tools, unconventional explosives and incendiary devices (home-made).	Simple and special tools, unconventional explosives and incendiary devices, (ABCR) weapons, with no regard for human life (including the perpetrators' own lives).

	Risk category 1	Risk category 2	Risk category 3
Types of perpetrators:	Outside companies: Radical groups; criminals enlisted by others; violent individual perpetrators Inside companies: Personnel; dismissed former employees; employees of other companies and visitors	Individual perpetrators, groups of perpetrators, possibly from the field of “organised crime”, radical political groups.	Extremist and terrorist individual perpetrators and groups.
Comments / Examples:	Deactivation of security devices, interference with production processes, failure to provide notification of critical system statuses, arson, vandalism following failed break-in, arson based on other motives.	Attack using fire/explosives, destruction of important operational facilities, interference with control systems incl. incorrect programming of control processors.	Armed attack, use of explosives at busy locations, rocket fire, setting fire to large facilities, attacks on plant security personnel, specific attacks on particularly sensitive areas, use of biological/chemical weapons, radioactive contamination with explosive devices (“dirty bomb”)

4.

Authorities / Institutions to be contacted

In addition to the possibility of undertaking technical and organisational improvements in the area of security, a further particularly important factor is **good and close cooperation** between the operators of critical infrastructures and the security and hazard control authorities.

The competent authorities and institutions should be consulted in matters of baseline protection, in order to involve them in an effective manner in the process of gathering information on risks and selecting appropriate measures. With regard to hazards relating to natural events, human error or technical failure, for example, authorities and establishments responsible for regional development and planning and for geology and weather information, disaster management and fire protection authorities, regulatory authorities, public order agencies, building authorities, immission control authorities, health authorities and environmental authorities are to be contacted at an early juncture. The initial direct points of contact for companies and operators of critical infrastructures are the authorities at local government level and the Land authorities.

The **Federal Office for Civil Protection and Disaster Response (BBK)** discharges duties for the Federation in the areas of civil protection and disaster response. The BBK pools all areas of civil protection measures via an

interdisciplinary approach to establish an effective protection system for the population and their basic necessities of life. As a “network node”, the **Centre for the Protection of Critical Infrastructures** at the BBK is responsible for disseminating information on and instilling an appreciation of the importance of critical infrastructures to the state and society, establishing cooperation between authorities and companies, developing analysis and protection concepts and proposing short-, medium- and long-term measures for the protection of critical infrastructures.

The **Federal Agency for Technical Relief (THW)** provides technical support in the area of civil protection and in dealing with disasters, public emergencies and major calamities. The THW acts on request from the bodies responsible for hazard control, its remit including duties in the areas of technical hazard control, technical relief in the area of infrastructure, technical relief in the field of environmental protection and public welfare in case of disasters.

Where external support, e.g. from the police, is required for the purposes of protection against **interference by unauthorised persons**, the operator should contact the competent local authorities prior to any such attacks occurring.

As a general principle, the Länder are also competent here with regard to matters concerning hazard control and preventive measures and in case of concrete investigations. The **Federal Police** (formerly the Federal Border Police - BGS) is the point of contact in matters regarding security measures for railway installations, airports and borders. The competence for investigations only lies with bodies such as the **Federal Criminal Police Office** (BKA) in isolated cases, such as instances of serious computer crime pursuant to Section 303b of the German penal code, when “there are actual indications that the offence is aimed at a) the internal or external security of the Federal Republic of Germany or b) security-critical points of vital facilities, the failure or destruction of which is likely to entail a substantial threat to people’s lives or health, or which are indispensable in order

for the community to function." In special situations, e.g. when duly commissioned by political bodies or the Federal Public Prosecutor, the BKA is involved in investigations for which it is not actually competent according to Section 4 of the law on the Federal Criminal Police Office and cooperation between federal and state authorities in criminal police matters (Federal Criminal Police Act).

The **Federal Office for Information Security (BSI)** is concerned specifically with matters of **IT security** in the information society. As the Federation's central IT security service agency, the BSI provides information on risks and hazards involved in the use of information technology, develops criteria and procedures for assessing and evaluating the security of information technology systems and advises manufacturers, distributors and users in all matters relating to security in the field of information technology.

Appendix 1

Questionnaire and checklist sample

The baseline protection concept can only be implemented if theoretical knowledge on hazards, threats and risks are operationalised by means of corresponding management concepts. Both questionnaires and checklists which are easy to work through are increasingly being used as tools for the operationalisation of security concepts at international level.

This questionnaire and checklist are thus to be regarded as a **sample** which is intended to provide a basis on which to implement the baseline protection concept independently and in a practice- and user-oriented manner. The questions are primarily intended to initiate and steer an **intra-company discussion process** on how to enhance security in a targeted manner. The checklists are designed as a concrete aid and control tool for use in the course of implementation.

Questionnaire

The questionnaire is non-exhaustive but should, like the checklist, be expanded and developed on a cooperative basis.

Structures and cooperation projects (organisation and management)

1. How are security aspects at the company structured and organized? What relations and cooperative structures exist or are planned between physical security, IT security and personnel security?
2. How does the company cooperate with other businesses in the field of security, including other

infrastructure users, such as in regional associations, and with private providers of services to be outsourced?

3. What security measures and cooperation structures exist or are planned in the field of up- and down-stream elements of the valued-added chains? What other cooperation arrangements are in place to cope with major incidents? What arrangements apply with regard to cooperation with involved security authorities and rescue and disaster management organisations, and how is such cooperation evaluated?

4. Which company units, institutions of the relevant business sector and supervisory authorities and which external institutions are concerned with the analysis of cases of damage (reconstruction of causes, conclusions, implementation of measures and monitoring of success) and, on the basis of such analysis, with further development measures, e.g. in the field of technical security?

Investigations, concepts (analysis of protection requirements)

5. Which specific security concepts exist for especially sensitive areas? According to which criteria are these areas identified and classified? Has a protection level been established? What conclusions do comparative studies draw with regard to international concepts and developments?

6. What studies and concepts exist regarding the substitution of services in case of large-scale damage?

7. What approaches are applied to quality management and risk management and what experience has been acquired in this area to date? How important is security management in the business optimisation concept?

8. What risk analyses are available, who has commissioned them and who has carried them out? What concepts exist for in-depth inter-system analysis and the development of measures with regard to interdependencies?

9. Are cost/benefit analyses carried out regarding the use/introduction of security measures?

10. Which incidents are registered and recorded? What information can be provided on unrecorded incidents (estimated number of unreported cases)?

Prevention measures (internal, external and personnel protection)

11. What key steps have been undertaken following especially serious incidents relating to the company's core business in the past (perhaps worldwide)?
12. What instruments are used in technical surveillance, investigations and evidence gathering? How effective have these measures proven?
13. What technical and organisational measures are used to protect a) the products and b) the production processes/facilities against abuse?

Crisis management for major incidents (contingency planning, redundant capacities, emergency plans)

14. How are incidents dealt with, e.g. escalation channels, risk assessment, decision-making powers etc.? Are there sector-specific approaches and instructions in place to differentiate cases of damage and for handling incidents?
15. What optimisation measures require to be carried out a) from the point of view of the authorities and organisations charged with security tasks (BOS) and b) by these authorities and organisations with regard the capacity to respond to major incidents?
16. What exercises on the management of major incidents have been carried out so far or are planned?

Sample baseline protection checklist

Similarly to the questionnaire, the following checklist is also intended as a concrete aid to implementing the baseline protection concept. Since special aspects relating to individual locations and situations cannot be taken into account here, the aspects covered in this checklist must be

adapted and supplemented according to the specific needs of the case concerned; similarly, further security measures may also be imperative. Consequently, the checklist also constitutes only a **non-exhaustive sample.**

The checklist comprises protection measures in the following areas:

1. **Protection of facilities and installations**
2. **Personnel**
3. **Organisation**
4. **Risk management**
5. **Emergency planning and contingency planning**

Protection of facilities and installations
(Location of the premises, structural design, inner perimeter,[4] protection of buildings)

	Yes	No	Plan-ned	Action required/ measures
Location of the premises concerned				
Can a threat to the company through severe natural events be ruled out?				
Flooding				
Storm tides				
Earthquakes				
Earthslides and hillside landslides				
Avalanches				
Storms				
...				
Is the area surrounding the company clearly structured and is the distance to neighbouring buildings sufficient in order to detect illegal entries (*open-plan building*)?				
If not, is the company shielded against neighbouring external buildings in such a way that it is difficult for intruders to gain unauthorised entry (e.g. via neighbouring roofs) (*closed design*)?				

[4] The *inner perimeter* is the area between the site boundary and the building boundary.

	Yes	No	Plan-ned	Action required/ measures
Structural design				
Are the company premises well-developed for traffic purposes and do they have a main exit and an emergency exit or exits which is/are independent of the main exit?				
Is the building protected against unlawful and possibly forced entry by means of structural elements?				
Bollards				
Concrete elements				
Barriers				
...				
Are there public parking spaces outside the premises (public area)?				
If so, is the distance from the buildings to be protected sufficient?				
Are parts of buildings to be protected situated outside of exposed locations and especially endangered areas?				
Are building frontages smooth and without projections?				
Are lightning conductors and other attachments designed in such a way that they cannot be used as climbing aids?				
Are rainwater pipes concealed under plaster or facing?				

	Yes	No	Plan-ned	Action required/ measures
Are telephone lines and other utility lines (e.g. electricity, oil/gas/water) installed underground and designed such as to exclude the possibility of manipulation?				
Are there any external sockets which can be switched?				
Inner perimeter				
Is the company's site enclosed?				
Is the enclosure without gaps?				
Is the enclosure designed in a straight line?				
Is the enclosure relatively resistant to breaching?				
Is the enclosure free of any elements which might facilitate climbing up or over the enclosure (e.g. diagonal members, adjacent trees)?				
Does the enclosure have a sufficient minimum height?				
Is there additional protection to prevent climbing over (e.g. projecting beams with barbed wire)?				
If the enclosure consists of fences, have precautions been undertaken to prevent intruders crawling underneath?				
If so, is the barrier concerned designed such that it cannot be used to facilitate climbing (e.g. concrete base, concrete kerbstones)?				

	Yes	No	Plan-ned	Action required/ measures
Are gates and doors within the enclosure (e.g. the fencing) designed in accordance with the height and intrusion resistance of the enclosure?				
Are there technical access controls in place (e.g. through a sliding/folding gate with protective measures to prevent climbing over, possibly performing a lock function [double gate], identity card readers and/or keyboard code, CCTV technology, two-way intercom system)?				
Is an electronic surveillance system in place to automatically detect any attempts to overcome the enclosure/access points (e.g. in the form of alarm fences/gates, CCTV technology with sensors, wall coping sensors, radar CRT, high-frequency light barriers, intrusion detection technology)?				
Is there shadow-free outdoor lighting?				
Are the lighting fixtures protected against damage (e.g. by means of screening glass or fine-meshed basket protectors)?				
Is underground cabling used for the power supply to the outdoor lighting?				
Is the enclosure monitored by video cameras?				
If so, does the company have appropriately trained security personnel to watch the video monitors who are capable of responding in an appropriate manner?				
If security guards are on site, do they also carry out patrols?				

	Yes	No	Plan-ned	Action required/ measures
Are thermal-imaging cameras/night-vision devices used?				
Are critical points/buildings (parts of buildings) subject to additional patrols?				
Is there a sufficient distance between greenery on the site (in particular trees, high bushes) and doors, steps, first floor and cellar windows?				
Protection of buildings				
Is there external screening of sensitive parts of the buildings?				
Do you avoid indicating parts of buildings which require protection (e.g. signposts, door plates)?				
Are special security areas required within the facility?				
Are these areas sufficiently protected by electronic and mechanical means?				
Have special access rights been defined for these areas (locking concept, technical access control)?				
Are persons entering or leaving sensitive areas monitored separately?				
Have external doors, accessible windows and light wells been integrated into an intrusion detection system?				
Are cellar windows equipped with certified security grids (corresponding to resistance class 5 at least in accordance with DIN 18106)?				

	Yes	No	Plan-ned	Action required/ measures
Are light shafts equipped with robust covering grid plates and lockable or firmly bolted devices to prevent lifting?				
Are the openings of supply and waste disposal shafts whose diameters exceed 30 cm provided with grids?				
Are roof domes/dome lights protected by mechanical and electronic means?				
Do the buildings have certified intrusion-resistant windows (in accordance with DIN ENV 1627)?				
Do windows in lavatories and other rooms where windows are typically often in a tilted position fitted with protective bars?				
Are the windows made of safety glass (projectile-resistant A glazing, intrusion-resistant B glazing, bullet-proof C glazing or explosives-proof D glazing)?				
Are windows without bars equipped (where technically feasible) with intrusion-resistant fittings of at least resistance class WK 5, projectile-resistant laminated safety glass (in accordance with DIN EN 356, resistance class P 6 A), lockable window handles and screwed-on glazing retaining strips?				
Are the doors leading outside limited to an expedient number?				
Do all external doors comply with resistance class WK 5 in accordance with DIN ENV 1627 at least?				

	Yes	No	Plan-ned	Action required/ measures
Does the main entrance door have – a card or chip reader?				
– interconnectable, self-locking bolts?				
– electronic security-door openers with a pressure resistance of at least 15000 N?				
– automatic door closers?				
– an external door knob (if electronic door-openers are used)?				
– a two-way intercom video system?				
Are emergency doors equipped with self-locking panic locks and automatic door closers and door sensors with a local alarm function?				
Are the main entrance and all other access points permanently locked during the day and can they only be opened by authorized staff?				
Is the main entrance equipped with a "deadman" door (such as a turnstile or a system of revolving doors consisting of metal or glass constructions) or a lock?				
Are entrances and exits separate from each other?				
Is clearance for authorized persons effected via electronic access rights (cards, transponders)?				
If so, are electronic access cards produced, stored, administrated and issued centrally?				
Have precautionary measures been undertaken to rule out the possibility of simply tracing the card back to the company?				

	Yes	No	Plan-ned	Action required/ measures
Are [a large number of] keys given exclusively to authorized personnel?				
Are the production, storage, administration and issuance of keys regulated centrally?				
Are spare keys available from specialist outlets only after presenting a security card?				
Are reserve keys stored in secure conditions?				
Are electronic access rights and keys only issued subject to the signing of a receipt (accompanied by appurtenant documentation)?				
Are locking rights checked promptly when areas of authorisation alter or employees leave the company?				
Fire protection				
Is a lightning protection system (external lightning protection) in place in accordance with DIN/VDE 0185?				
Are existing fire protection regulations (e.g. DIN 4102) and stipulations by supervisory authorities for buildings complied with?				
Has the local fire brigade been consulted in planning fire protection measures?				
Is there a danger alarm system whose signals/alarms are relayed to a permanently manned unit (reception, gate, guards and security service, fire brigade, etc)?				

	Yes	No	Plan-ned	Action required/ measures
Further protection measures				

Personnel (employees, outsiders[5])				
	Yes	***No***	**Plan-ned**	**Action required/ measures**
Personnel (internal and external)				
Is security vetting carried when recruiting new personnel?				
Is security vetting carried out on external staff who are to be employed (temporarily)?				
Is security vetting carried out to counter sabotage among the personnel in accordance with the German Security Clearance Check Act (SÜG)?				
Are the personnel obliged to comply with applicable laws, provisions and internal regulations (e.g. Section 5 of the Federal Data Protection Act ("data secrecy")?				
Has an awareness of security issues (terrorism, sabotage) been instilled in the personnel?				
Outsiders[2]				
Are outsiders required to report to the reception/gate /guards?				
Are outsiders quickly and easily identifiable (e.g. by means of visitor I.D. cards)?				
Are outsiders escorted / supervised?				

[5] *Outsiders*: e.g. visitors, craftsmen, maintenance and cleaning personnel.

	Yes	***No***	**Plan-ned**	**Action required/ measures**
Are checks carried out on suppliers and incoming goods?				
Further protection measures				

Organisation (within the company, outside of the company)				
	Yes	**No**	**Plan-ned**	**Action required/ measures**
Within the company				
Does your company have an appropriately trained security officer?				
Are security personnel belonging to the company responsible for the facility to be protected?				
Are the company-employed security personnel familiar with the legal provisions and specific duties and powers required for the discharge of their duties and practical application of such provisions and powers (through instruction pursuant to Section 34a of the German industrial code (GewO)/Section 4 of the German ordinance on guard services (BewachV))?				
Are the legal requirements and/or standards relevant to security clear?				
Are security requirements duly defined (guidelines, directives)?				
Are the personnel informed and regularly trained in operational security requirements?				
Are security-relevant incidents recorded?				
Have consequent steps been taken following security-relevant incidents?				

	Yes	No	Plan-ned	Action required/ measures
Do the personnel possess a basic understanding of the areas of occupational safety, fire protection and "first aid"?				
Have potential sources of danger and early warning indicators been identified?				
Is there a concept in place for the classification of critical locations and business processes?				
Is there a security centre at locations which are classified as critical?				
Does your company keep a register of hazardous substances?				
Are there exact layout plans of all supply and discharge lines (e.g. electricity, water, sewage, gas, telephone, alarms)?				
Are there plans for graduated security measures (depending on the current threat situation)?				
Is there an escalation strategy in place for security incidents?				
Is there an alert plan?				
Are there rules of conduct and reporting channels in place for security incidents?				
Do the personnel receive regular instruction on escape routes?				
Are evacuation exercises carried out regularly?				
Are fire protection exercises carried out regularly?				

	Yes	No	Plan-ned	Action required/ measures
Are findings from exercises incorporated into training concepts?				
Is a crisis communication system in place (information to employees, points of contact for authorities and the media)?				
Are there provisions for psychological care of affected personnel in the event of security incidents?				
Outside the company				
Is there a so-called disaster communication line (priority line for specific telecommunications)?				
Is security managed exclusively by the company itself?				
If not, do contractors/external security providers comply with DIN 77200 Level 3?				
Has this system proven effective from the point of view of the company's management?				
Are there agreements in place between the company and security providers (contractual arrangements, practical cooperation, areas of responsibility in the event of crises)?				
Are the security personnel familiarised with the specific situation at the company and do they receive ongoing training?				
Has the critical nature of outsourced services been assessed in terms of the company's functionality?				

	Yes	No	Plan-ned	Action required/ measures
Are open sources which could pose a threat to the company (e.g. aerial photographs on the internet, production materials and quantities, distribution channels etc.) avoided?				
Further protection measures				

Risk management				
	Yes	**No**	**Plan-ned**	**Action required/ measures**
Has a binding risk policy been defined for the entire company?				
Is there a specific risk policy in place for individual areas within the company?				
Are all potential risks to the company identified and evaluated, including — risks from natural events, — risks from human error/technical failure, — risks from terrorism and/or criminal abuse?				
Are environmental risks (e.g. power stations, railway lines) considered?				
Are the target security standard and the accepted risk defined overall and according to risk categories?				
Are all risks within the acceptable scope of residual risks?				
Are risk management measures in place in all individual areas within the company (natural events, human error/technical failure, terrorism / criminal abuse), and are these coordinated?				
Are there appropriate instruments in place for regular risk monitoring (early warning systems, risk controlling)?				
Are decisions relating to risk financing based on medium-term and long-term cost/benefit analyses?				

Emergency planning and contingency planning

	Yes	No	Plan-ned	Action required/ measures
Do you have a manual for crises and emergencies?				
Are areas of responsibility in the event of an emergency defined?				
Are there crisis and emergency plans in place for selected incidents?				
Are emergency exercises carried out regularly?				
Are reporting channels and decision-making powers organised for possible incidents?				
Are cooperative arrangements with the competent authorities in place for major incidents?				
Have crisis and emergency plans been agreed with the competent authorities?				
Is sufficient emergency power capacity available, also covering the security installations?				
Have technical and organisational fire protection measures been undertaken? Fire extinguishers				
Fire alarm systems				
Personnel training				
Escape routes				

	Yes	No	Plan-ned	Action required/ measures
Examination				
...				
Are exercises carried out on handling major incidents (with the involvement of the competent authorities)?				
Is technical and organisational protection in place to prevent failures in the production process?				
Are studies and concepts available regarding the failure of external services in case of major incidents?				
Are redundant capacities available?				
Are there concepts for the resumption of services/ production following incidents (Business Continuity Management - BCM)?				
Further protection measures				

Appendix 2

Police information

There are three publications which the section specialising in “Offences involving explosives and fires” at the Federal Criminal Police Office (BKA) has drawn up for the Land criminal police offices and affected companies. These contain information on initial measures in case of bomb threats and on procedures on receipt of mail which is suspected of containing explosives or biological or chemical agents. The publications are available from the competent Land criminal police offices (see addresses p. 76).

In view of the substantial danger which such mail poses to people, precautionary measures should be planned to minimise the level of risk. In addition to basic staff training, such measures include regular exercises, clearly defined areas of responsibility and, where necessary, modifications to buildings (mailrooms separated from other facilities).

Note:

In the event of a bomb threat, always call the emergency police number!

Every bomb threat is to be taken seriously, and final assessment - on the basis of the information and impressions acquired by the recipient of the bomb threat - should be carried out by the police.

Land Criminal Police Office of Baden-Württemberg
Taubenheimstr. 85
70372 Stuttgart

Land Criminal Police Office of Mecklenburg-Vorpommern
Retgendorfer Str. 2
19067 Rampe

Land Criminal Police Office of Schleswig-Holstein
Mühlenweg 166
24116 Kiel

Bavarian Land Criminal Police Office
Maillingerstraße 15
80636 Munich

Land Criminal Police Office of Lower Saxony
Schützenstraße 25
30161 Hanover

Land Criminal Police Office of Thuringia
Am Schwemmbach
99099 Erfurt

Land Criminal Police Office of Berlin
Platz der Luftbrücke 6
12101 Berlin

Land Criminal Police Office of North Rhine-Westphalia
Völklinger Straße 49
40221 Düsseldorf

Land Criminal Police Office of Brandenburg
Tramper Chaussee 1
16225 Eberswalde

Land Criminal Police Office of the Rhineland Palatinate
Valenciaplatz 1-7
55118 Mainz

Land Criminal Police Office of Bremen
In der Vahr 76
28329 Bremen

Land Criminal Police Office of the Saarland
Hellwigstraße 14
66121 Saarbrücken

Land Criminal Police Office of Hamburg
Bruno-Georges-Platz 1
22297 Hamburg

Land Criminal Police Office of Saxony
Neuländer Straße 60
01129 Dresden

Hessian Land Criminal Police Office
Hölderlinstraße 5
65187 Wiesbaden

Land Criminal Police Office of Saxony-Anhalt
Lübecker Str. 53-63
39124 Magdeburg

Appendix 3

Excerpt from:

Für den Notfall vorgesorgt
(“Provisions for emergencies”)

An information brochure from the

Federal Office for Civil Protection and Disaster Response

Information correct as per: August 2004

The complete brochure is available at
http://www.bbk.bund.de (*background information and tips for the public).*

Note:
The brochure “Für den Notfall vorgesorgt” is intended in particular for the general public and the individual citizen. The information contained in the brochure on dangers from natural events and technical accidents and the tips on precautionary measures can also be used in modified form for corporate precautionary planning, however.

Introduction

Accidents and disasters are in the news every day. Anyone can be affected by large-scale fires, flooding, chemical accidents, power failures (energy failures) or suddenly arising dangers.

An extensive emergency response system is available to citizens as a comprehensive means of averting such dangers. While the fire brigade and rescue services are on hand to provide daily support, the Länder operate disaster management systems to counter disasters and the dangers which are inherent to the high-tech, highly automated world in which we live. The Federation reinforces and consolidates the integrated emergency response system for large-scale emergencies and crises by providing additional vehicles, helpers released from military service, rescue helicopters for civil protection operations and through the Federal Agency for Technical Relief. The Federation, Länder and local authorities thus cooperate on a partnership basis in the field of civil protection and disaster response to provide citizens with assistance in emergencies. But time passes until assistance arrives - valuable time in which a matter of minutes may decide the fate of people’s lives, property or assets. Minutes in which each of us may be forced to act on our own initiative.

It is too late for extensive precautionary measures when an emergency has occurred - now is the time for such measures to prove their worth. It is too late to learn the correct way to respond to fires or accidents when a fire has already broken out or an injury has been sustained. We can only help if we have prepared for an incident before it actually occurs, by learning first aid, refreshing this knowledge regularly and acquainting ourselves with the appropriate precautionary measures to deal with dangerous situations or crises.

So be prepared! The sooner the better, as no-one can predict when they might face a danger! Establishing a solid

foundation for coping with possible emergencies often requires only a little time and effort.

Dangers resulting from extreme weather

Extreme weather conditions can arise so suddenly as to render due preparation virtually impossible. Follow the weather reports and warnings. This can reduce dangers and prevent or minimise damage. Loose branches, trees and roof tiles can always pose a danger in extreme weather. Roads may be flooded in heavy rain. Damage to the carriageway or drain covers lifted by the pressure of the water can subsequently become a danger to vehicles and pedestrians. Notify the fire brigade if hazardous substances such as fuel oil have been released.

As general precautions, you should have the following to hand in extreme weather situations:

- A battery-powered VHF radio with sufficient batteries
- Battery-powered light sources such as torches and candles
- Emergency baggage containing important documentation, should you have to leave your home.

Tip:

The documentation should include photographs or similar of your property. This may be of great assistance to insurance agencies, should your property incur damage.

Thunderstorms involving lightning discharge entail additional dangers. Note the following precautions here:

- Avoid tall trees, masts, aerials and similar. Seek shelter in a building.
- Remain in your vehicle and do not touch any bare metal parts.
- Remain at a distance of at least 50 metres from overhead power lines.
- Lightning may result in excess voltage levels. Do not rely entirely on your home's lightning protection system. Disconnect sensitive devices from the mains or use appropriate overvoltage protection devices.
- Lightning striking masonry can cause substantial damage and give rise to cracking or fracturing.

Heavy thunderstorms sometimes give rise to **hail** and **hurricanes.** Additional sources of danger are hailstones and debris and dirt which are entrained by the violently rotating funnel of a hurricane. Note the following precautions in case of hail and hurricanes:

- Close door or window shutters, keep away from unprotected openings.
- Go to a low-lying room, e.g. cellar, or a room situated in the building's interior; cars, caravans and lightweight constructions may not offer adequate protection.
- Avoid rooms with large roof spans, e.g. halls.
- Do not remain outside! Go to a solid building! If needs be, lie down with your face to the ground and protect your head and neck with your hands!

Procedure after extreme weather

- Check your general area for damage such as water intrusion or glass breakage, etc.
- Only put electrical devices into operation if they have not come into contact with moisture.
- If someone is injured, administer first aid and call the emergency services.

- If the building is damaged, leave it and do not re-enter it until it has been classified as safe by specialists.
- If the roof is damaged after a storm, keep away from the area in which it might collapse. This area corresponds to one third of the height from the floor to the gutter. Notify the fire brigade.

Flooding

In recent years, flooding has become an increasing threat to the basic necessities of life for parts of the population. In addition to the efforts undertaken by the Federation, the Länder and local government authorities to limit the consequences of such incidents, individuals should also examine how they can prevent or reduce resultant damage by means of specific preparations and measures. The following tips and information may be of assistance here. As an initial step, you should ascertain the critical high-water mark from your local authority.

Please consider that the normal supply of electric power, food and drinking water may be impaired or interrupted at times of flooding. This state of affairs may continue for a while after the immediate effects of flooding have passed, owing to damage to the infrastructure.

Particular hazards apply during **flooding** as a result of the massive erosive impact of water on roads, bridges, dams etc. and from flotsam. Leaking harmful substances such as fuel oil, detergents and pesticides, faeces and refuse which are carried off in the floods pose a health risk. Drinking water may be contaminated.

The following **preparatory measures** are recommendable:

- Keep boarding, waterproof plywood panels and silicon to hand to seal off rooms which are at risk, as well as sandbags.
- Transfer hazardous substances or chemicals to another location in good time.

- Remove valuable furniture or equipment from rooms which are at risk.
- Use waterproof building materials and carry out sealing work in rooms which are at risk.
- Secure fuel tanks to prevent them from floating free and being carried away by flood water (vertical rear anchorage/use of ballast, e.g. earth coverage in case of impending danger). If possible, use tanks which are suitable for applications involving water pressure from outside. Prepare facilities for shutting off piping.

Safety precautions:

- Make plans for the care of people who are ill or in need of help. Organise arrangements for timely “evacuation” to relatives or friends outside of the danger zone.
- As landline and mobile telephone networks may fail in crisis situations, arrange emergency and danger signals with neighbours and the fire brigade.
- Inform each member of the family about precautionary measures undertaken to counter dangers, correct responses and key elements of individual preparedness. Discuss the assignment of responsibilities in emergencies (operation of mains switch and shut-off valves, safeguarding of documents, etc.).

In case of impending flooding:

- Follow the latest weather reports and flood warnings via regional radio stations, teletext and regional television stations. Inform other occupants of the house as appropriate.
- Check the precautionary measures undertaken and carry out any appropriate additional measures.
- Clear out rooms which are at risk.
- Seal up doors, windows, drain openings, etc. which are at risk.
- Carry out appropriate safety measures for heating and electrical devices in rooms which are at risk or switch

such devices off. Condensation water is sufficient to pose a risk of electric shock! Take due account of the freezer.

- Check house drainage systems and flap traps in the cellar.
- Remove vehicles from endangered garages or parking spaces in good time.
- Notify the fire brigade of any leakages of harmful substances.

Additional note on motor vehicles:

- Do not drive on flooded roads. Water entering into the engine compartment may cause serious damage; in addition, a catalytic converter operates at around 700°C and sudden cooling may cause the ceramic head to shatter.
- Never start a vehicle which is up to the oil sump or up to its wheels in water. Arrange for it to be towed away and checked at a garage.

Save lives:

- Saving human life has priority over protecting property and assets.
- Never undertake any rescue attempts without ensuring your own safety - call for help!
- Do not approach the banks of rivers, as there is a risk that they may cave in and you may be carried away! The same applies to driving on flooded or partially flooded roads! Observe barriers blocking off roads and follow the instructions issued by the local authorities and the emergency services!
- Do not “cruise” along on flooded waterways, as this will cause waves and underwater obstacles constitute a danger!

After flooding

- Remove residual water and sludge, but do not pump the affected rooms dry until the floodwater has receded and

the groundwater level has fallen sufficiently. Observe the information provided by your local authorities.

- Floor coverings and clothing should be removed or opened for inspection purposes.
- Dry affected areas as quickly as possible, in order to counter structural damage, mould or other forms of infestation. Heating devices can be used to support the drying process.
- Have damaged structural components of the building examined (statics).
- Do not put electrical devices and systems back into operation until they have been checked by a specialist.
- Have fuel oil tanks checked for damage.
- Notify the fire brigade if hazardous substances such as pesticides, paints, lacquers, detergents or fuel oil have been released. Disposal may have to be carried out by specialist companies.
- In case of leaked oils, use oil binding agents only in consultation with the fire brigade.
- Rooms in which work is carried out should be well ventilated at all times. If hazardous substances have been released, do not smoke and avoid open fire.
- Dispose of soiled furniture and foodstuffs.
- In case of gardens or fields covered with thick layers of oil sludge, notify the rural county office or the office of agriculture.

Information, tips and, where appropriate, the addresses of specialist companies are available from your competent local authorities and the fire brigade.

Tip:

Information on procedures in case of flooding and all other types of danger is available via the German Emergency Preparedness Information System (deNIS): www.denis.bund.de.

Energy failure

All the citizens of industrialised nations are reliant on various sources of energy today. These include electricity, gas, oil and district heating, which are delivered to the home via distribution networks. The possible consequences of a power failure show just how dependant we are on such supplies: All mains-powered devices fail. These may include:

- Water heaters
- Radios
- Lighting
- Cash dispensers
- Telephones
- Computers
- Mains-dependent door mechanisms and other mechanisms
- and much more besides.

Even heating systems are commonly reliant on electricity, including oil heating systems, as transportation of the oil through rising pipelines, injection and ignition all require electricity. Manual control of these functions, if possible at all, entails substantial and costly modification measures.

Energy supply tips:

Every household should keep alternative resources available, should the oil, gas, district heating or electricity supply fail. In our climes, a lack of heating can generally be compensated for over a certain period by warm clothing. Those who possess a means of heating which can also be operated with coal, briquettes or wood should keep a stock of such fuels for emergencies.

Should the electric lighting fail, candles, torches or petroleum lamps can be used instead. Here again, stocks of candles, fuels, spare bulbs for torches, batteries and lighting means such as matches or lighters should be checked.

Rechargeable batteries are less suitable as emergency supplies, as they do not retain the stored current sufficiently long in charged state and in the event of a power failure they would need to be fully charged. Please note that in unfavourable circumstances an energy failure may last several weeks.

Self-protection in the home

Although there is no such thing as absolute protection against all incidents or cases of damage, most dangers can be countered by preventive measures or harmful consequences can be diminished by effective action. It is particularly important, for example, to inform oneself in good time about any impending dangers at one's place of residence and the precautionary measures which have been undertaken.

The dangers to people and property can also be reduced substantially by measures of preventive fire protection in the home, e.g. by using fire-retardant building materials, fire-proof doors in boiler rooms, fitting smoke detectors and ensuring that fire-fighting devices are available.

Measures to combat fires

Around 600 people are killed and over 5,000 are injured by fires throughout Germany each year! Property to the value of over 10 billion euros goes up in flames in private homes every year. Disasters can lead to extensive fires. Fire protection thus forms part of the necessary precautionary measures. If, despite all precautions, a fire occurs, whereby many sources of fires may arise as a result of a disaster, the fire brigade cannot be everywhere at the same time. In this case, it is vital for those affected to respond quickly and in the correct manner, so as to ideally extinguish fires immediately after they occur. This requires a number of simple devices such as fire extinguishers or a garden hose, which should be kept in an easily accessible place.

Before a fire breaks out:

Irrespective of whether you are in your own home or another building, prior to a fire breaking out you should ascertain

- how the next stairwell is to be reached in case of danger (these stairwells are escape and rescue routes leading outside; lifts must not be used in case of fire!),
- what preparatory measures have been undertaken to evacuate people with walking difficulties,
- what facilities are available for making an emergency call,
- where fire extinguishing devices are located and how they are operated.

Please ensure

- that corridors and stairwells are not narrowed or even blocked by any objects - it must be possible to use the escape route free of any obstacles,
- that doors along rescue routes are closed but never locked, in order to counter spreading of the fire or smoke along the escape route,
- that hydrants and fire brigade access routes are not blocked,
- that the building’s safety facilities are not damaged and that any damage is reported immediately,
- that open light, candles or fire are kept under surveillance at all times,
- that the electrical systems and devices are in perfect working order and are not interfered with,
- that the most important documents and papers are kept to hand at home, should “evacuation” unexpectedly be necessary.

Tips on fire prevention:

- In the cellar: Remove superfluous inflammable materials!
- In the loft: Clear the loft up, in particular removing inflammable materials from all corners or under the slope of the roof!

- Ensure that fire-fighting resources are available for emergencies, e.g. fire extinguisher, water hose, fire blanket, etc.!
- Have fire extinguishers serviced and tested on a regular basis!
- Learn how to operate fire extinguishers and how to use available fire-fighting resources correctly!
- Never leave open fire or similar sources of danger unattended!

If fire breaks out:

In order to facilitate your own rescue and the rescue of others in a fire, you should have a knowledge of the right self-protection procedures. People's safety has absolute priority. If you discover a fire, you should observe the following sequence of actions:

If the fire is only just starting, carry out initial extinguishing attempts immediately to "nip it in the bud".

- Only attempt to extinguish the fire if this does not involve you endangering yourself!
- Never use water to extinguish burning fat or other liquid fuels.
- If electric current poses a threat, switch off the power supply in the affected area before beginning your extinguishing attempts!
- Extinguish from bottom to top and from the sides towards the middle!
- Never enter smoke-filled rooms. Fatal fire gases form in such conditions. Close the door and alarm the fire brigade.

If it is not possible to attempt to extinguish the fire: Close the windows in the room, if you can do so without putting yourself at risk, and also close the door of the room in which the fire is burning. This will deprive the fire of oxygen.

Call the fire brigade!

Warn other persons and get them to safety (or arrange for others to do so).

Wait for the fire brigade and brief them on arrival, or arrange for another person to brief them.

Until the fire brigade arrives, you should try to prevent the fire from spreading. Keep the door to the room in which the fire is located damp to prevent the fire from burning through or to delay the same.

If you have to leave the building or the flat, storey, etc., ensure that no-one stays behind. Doors to rooms in which there is no fire should remain unlocked to facilitate quick searches; fire-proof doors and fire compartment doors are to remain closed, of course. Do not lock any doors! Keep the keys for rooms or windows which are only accessible with keys available for the emergency services.

Outside of the danger zone you should ascertain whether all the occupants of the house are in safety, as when a person is missing the fire brigade always has to assume that the person concerned may be in the building and thus in danger.

You should respond to a test alarm (e.g. at your workplace) in the same manner as you would respond to a real fire. Should you one day take a “real” fire alarm to be a test and fail to respond, this may place you and the emergency services in danger.

Further information is available from your local fire brigade!

Hazardous substances – Protection principles

Hazardous substances may be released in industry, when transporting hazardous materials, and even in the home. The scenarios range from the careless handling of cleaning agents through accidents to a crisis situation in which such substances may pose a threat to our health. Radioactive and toxic chemical substances occur as gases, fumes and dust particles. When released, such substances can pose a threat to people, depending on the type of substance and the amount released.

The individual citizen is not generally able to identify whether a dangerous situation applies which requires special protection measures for the population. In such cases, you should heed the announcements and recommendations from the authorities, which are broadcast via radio and public address systems. A number of simple rules of conduct provide for enhanced protection in certain dangerous situations and can help to reduce dangers.

Self-protective behaviour in case of risk of radioactive contamination:

1. **When outdoors:**
   - Go to the nearest inhabited house.
   - Try to move at right-angles to the wind direction, breathe through a breathing mask if possible, but use a handkerchief at least.
   - If you have already come into contact with radioactive substances, change your outer clothing and shoes on entering the house.
   - Leave contaminated outer clothing and shoes outside of the living area.
   - Wash your face, hair, hands, nose and ears thoroughly.
   - Follow the instructions which apply in buildings.

2. **When travelling by car:**
   - Switch off the ventilation and close the windows.
   - Listen to the radio (VHF, regional stations) and follow the instructions from the authorities and emergency services.
   - Otherwise, drive to the next inhabited building, observing the instructions under 1. on arrival.

3. When in a building:

- Remain in the building.
- Give endangered passers-by temporary shelter.
- Inform other occupants of the house, if necessary.
- Close doors and windows.
- Switch off fans and air conditioning, close the ventilation slots in window frames.
- Go to a cellar room or a protected room inside the home, preferably without any outside windows.
- Avoid unnecessary consumption of oxygen by candles or similar.
- For information purposes, tune the radio to a regional VHF station or switch on the television.
- Heed the announcements by the authorities and emergency services.
- Use the telephone in emergencies only.
- Should radioactive particles enter the building, use available breathing equipment, if needs be mouth protection in the form of a surgeon's mask or cloths.

Self-protective behaviour in case of biological or chemical hazards:

1. When outdoors:

- Go to the nearest inhabited house.
- Try to move at right-angles to the wind direction, breathe through a breathing mask if possible, but use a handkerchief at least.
- If you have already come into contact with hazardous substances, change your outer clothing and shoes on entering the house.
- Leave contaminated outer clothing and shoes outside of the living area.
- Wash your face, hair, hands, nose and ears thoroughly.
- Follow the instructions which apply in buildings.

2. When travelling by car:

- Switch off the ventilation and close the windows.
- Listen to the radio (VHF, regional stations) and follow the instructions from the authorities and emergency services.
- Otherwise, drive to the next inhabited building, observing the instructions under 1. on arrival.

3. When in a building:

- Remain in the building.
- Give endangered passers-by temporary shelter.
- Inform other occupants of the house, if necessary.
- Close doors and windows.
- Switch off fans and air conditioning, close the ventilation slots in window frames.
- Go to a well protected room inside the home, preferably without any outside windows.
- Avoid cellars or other low-lying rooms.
- Avoid unnecessary consumption of oxygen by candles or similar.
- For information purposes, tune the radio to a regional VHF station or switch on the television.
- Heed the announcements by the authorities and emergency services.
- Use the telephone in emergencies only.
- Should toxic chemical substances enter the building, use available breathing equipment, if needs be mouth protection in the form of a surgeon’s mask or moist cloths.

Everyone should be able to help themselves and others until assistance from the organised specialists arrives. First aid is an important element of self-protection. Relief organisations will be pleased to provide you with details of the locations and times of available courses.

Civil protection and disaster control

Through the Federal Office for Civil Protection and Disaster Response (BBK), the Federation makes an important contribution to civil protection, pooling and integrating the capacities at Federation, Länder and local authority levels to establish an integrated emergency response system. The scope of resources available from the Federation includes civil protection helicopters for air rescue operations, ABC detection vehicles and the Federal Agency for Technical Relief as well as the BBK.

The local authorities are responsible for the area of self-protection. They are supported in this task by the BBK. The individual's capacity to help himself or herself provides the indispensable basis for organised assistance. Please address any questions relating to civil protection or self-protection to the

Federal Office for Civil Protection and Disaster Response (BBK)
Deutschherrenstraße 93-95 · 53177 Bonn
Telephone: (01888) 550-0, telefax: (0228) 5554-436
http://www.bbk.bund.de
info@bbk.bund.de

The Länder operate a disaster control system to support rescue services and fire brigades in connection with special or exceptional incidents, such as major accidents, technical and natural disasters which necessitate supra-local cooperation between emergency services. Organisations involved here include:

- the Workers' Samaritan Federation Germany
- the Deutsche Lebens-Rettungs-Gesellschaft (German Life-Saving Federation)
- the German Red Cross

- the fire brigades
- Johanniter-Unfall-Hilfe (St. John's Ambulance Brigade)
- the Malteser-Hilfsdienst (voluntary agency)
- the Federal Agency for Technical Relief.

In an emergency situation such as an accident, people may incur injuries and subsequently require help from others. Only in the rarest cases are emergency services or the fire brigade on the spot immediately. They require to be alarmed by an emergency telephone call. An effectively functioning and generally known emergency call and alarm system thus forms the essential basis for any form of organised assistance. The police, fire brigade or rescue service can be reached all over Germany on the following telephone numbers:

Fire brigade: 112 **Police: 110**

Please inform yourself about any additional local emergency telephone numbers. By the way, you can also call the 112 emergency number on your mobile telephone at any time without a card!

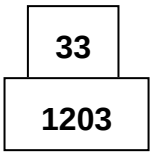
The time until the rescue service or fire brigade arrives must be bridged with self-protective measures. The list below shows the order in which such measures should be carried out:

1. Make the site of the incident safe, if necessary.
2. Carry out immediate life-saving measures.
3. Call help by dialling 112 or one of the other emergency telephone numbers.
4. When making the emergency call, you should state:
    - Where the incident has occurred
    - What has happened

- How many persons are injured
- What form the injuries take
- Await any questions from the responding service!

5. Administer first aid until the rescue service arrives.

If the incident concerns an accident with a vehicle transporting hazardous materials, please state the top figures on the orange-coloured warning panel on the vehicle.



Important telephone numbers

Police 110

Fire brigade 112

Rescue service

Emergency medical service

Poisoning emergencies

Pharmacy providing after-hours

Local department of works service

Emergency	Fire
Where has the emergency occurred?	Where is the fire?
What has happened?	What is on fire?
How many people are injured?	What is the extent of the fire?
What type of injuries?	What types of danger? (people in danger, stored gas cylinders or similar?)
AWAIT questions from the responding service!	AWAIT questions from the responding service!

Appendix 4

Glossary on baseline protection concept

BOS	Collective term in Germany for authorities and organisations performing security-related functions (police and disaster control authorities of the Federation and the Länder, Federal Customs Administration, fire brigades, THW technical support service, relief organisations).
Business Continuity Management (BCM)	All organisational, technical and personnel measures which serve to continue a company's core area of business directly after a crisis and to successively resume the entire scope of business activities in case of prolonged down-times or malfunctions.
CBRN hazards	Hazards of a chemical, biological, radiological or nuclear nature.
Contingency planning	Provisions to maintain or restore business processes in the event of unforeseen incidents or malfunctions.
Crisis	A suddenly or insidiously developing situation differing from the normal state of affairs and entailing a risk potential which harbours dangers and threats to life and limb or to significant material assets and serious risks to the political, social or economic system, and which requires a decision to be made, often in a state of uncertainty and on the basis of incomplete information.
Crisis communications	All communicative activities pursued in connection with a crisis. In practice, crisis communications entails the clear allocation of areas of authority and responsibility and a clear line of communication to ensure uniform content and cohesive argumentation. In this context, agreement is also necessary as to how the media are to be involved in presenting the crisis.

Crisis management	Establishment of conceptual, organisational and procedural basis to support the process of restoring a normal state of affairs as quickly as possible after the occurrence of an exceptional situation.
Criticality	Assessment of the extent and probability of failure of a critical infrastructure area/process.
Damage	Destruction and impairment of concrete or abstract assets. This includes impaired health, erosion of opportunities in life and quality of life and the loss of monetary assets. This category also includes forms of non-material damage, such as the loss of trust in the integrity of political decision-makers.
Damage by natural forces	Damage resulting from natural phenomena (e.g. fire, heat, lightning, flooding, storm tides, frost, avalanches, rockfall, earthquakes).
Danger	Possibility of an incident (natural phenomena, technical failure, human error, human misconduct) which may lead to injury or cause damage to material assets and the environment or result in social and economic disturbances.
Danger analysis	Method of identifying and evaluating regions, infrastructures, facilities and installations which may be at risk as a result of possible incidents.
Danger categories	Systematisation of individual dangers according to the initiating events.
DIN 18106	Requirements and test procedures for intrusion-resistant gratings.
DIN 4102	Behaviour in fire of building materials, building components and special building components.
DIN 77200	Basic requirements pertaining to the organisation, personnel management and working practices of security service providers.
DIN EN 356	Special security glazing/test procedures and classification of resistance to manual attack.

DIN ENV 1627	Requirements for and classification of intrusion-resistant doors and windows.
DIN/VDE 0185	Lightning protection/protection of premises and persons.
Dirty bomb	Conventional explosives to cause an explosion via which radioactive substances are dispersed.
Disaster	(Large-scale) emergency resulting from natural causes (earthquake, storm tides, volcanic eruption, etc.) or human activities (chemical accident, aircraft crash, attack, etc.) which may lead to an acute danger to the life or health of a large number of people, to the environment or to other significant objects of legal protection and which the authorities responsible for hazard control are unable to handle adequately with their own personnel and resources.
Domino effect	Sequence of events in which each individual event is the cause of the following event; all the events can be traced back to one and the same initial event.
Emergency planning	All concrete preparations for crises/disasters which are to be undertaken in order to ensure that they are handled effectively.
Hazard	(Concrete) effects of dangers/threats (natural phenomena, technical failure or human error, human misconduct) on critical infrastructures.
Hazard analysis	Method of identifying and evaluating the consequences of possible incidents on infrastructures, facilities and installations or the population in order to derive protection measures.
Hazard control	Measures to maintain or restore public safety.
Hazard control authorities	The authorities responsible for hazard control (police and authorities responsible for public order).
Infrastructures, critical	Organisations and facilities of great significance for the community whose failure or impairment would cause a sustained shortage of supplies, significant disruptions of public order or other dramatic consequences.[6]

[6] Definition of cricital infrastructures by the KRITIS working group at the Federal Ministry of the Interior (BMI) of 17.11.2003.

Interdependency	Interactions or mutual influences between different critical infrastructures.
ISO standard 17799	International standard on information technology security; directive on setting up and operating an information security management system (ISMS)
Ordinance on Major Incidents	Ordinance implementing the Seveso II Directive in German law; contains obligations for operators of operational areas within the meaning of Section 3 (5a) of the Federal Immission Control Act, stipulating measures to prevent incidents and modes of conduct after incidents have occurred.
Perceived risk	Risk assessment based largely on personal experience, communicated information and intuitive appraisal.
Protection objective	Description of a targeted state of affairs. Protection objectives are derived from the results of danger analysis and risk assessment.
Quality management	All measures undertaken by a company with the aim of establishing, assuring and improving quality. The scope and contents of quality management are commonly specified in a quality management manual, which should be drawn up in accordance with the ISO 9000 standards. Quality management is implemented at a company by means of a corresponding quality management system.
Redundancy	The multiple availability of identical resources in order to increase the fail-safeness of a system.
Risk	Likelihood of a serious danger which – constitutes a threat to human life, – will impair the health of a large number of people, – affects economic activity, public services and technical infrastructures and may cause damage to the environment, in particular animals and plants, the soil, the water, the atmosphere and cultural and material assets.

	The risk expectation is classified according to different levels - “very high”, “high”, “medium”, “low”, “minimal” and “very minimal”. It is dependent on the susceptibility of the region concerned to damaging impacts, e.g. of a natural, physical, technical, economic nature (vulnerability), and on the likelihood of an exceptional situation occurring. In mathematical terms, the risk, *r*, is defined as the product of the extent of the damage, *d*, and the likelihood of occurrence, *l*. $r = d \times l$
Risk analysis	Assessment of the danger potential and the susceptibility of a region/facility or installation to damaging impacts and determination of the resultant consequences (risk determination).
Risk assessment/evaluation	Method of judging a risk in rational terms, with due consideration to its acceptability for society as a whole or for certain groups or individuals. Scientific risk analysis and perceived risk as determined by empirical studies form part of the risk assessment process.
Risk management	The totality of measures to minimise the risk situation, weighing up the strategic alternatives (optional courses of action) in consultation with the parties concerned and according due consideration to the risk assessment and other factors worthy of consideration.

Appendix 5

For further reading (literature, Internet links)

The following references to literature, manuals, guidelines and internet addresses are intended as an initial aid and represent only a selection from the vast scope of printed and electronic information which is now available.

We welcome additional tips in order to broaden this information and keep the references up to date, particularly with regard to internet sources. Please send relevant details to: BBK-Zentrum-I@bbk.bund.de

1. Literature

Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzhandbuch (Stand: November 2004)
http://www.bsi.bund.de/gshb/deutsch/index.htm

Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (Hrsg.), Vollzugshilfe zur Störfall-Verordnung, März 2004
http://www.umweltministerium.de/files/broschueren/faltblaetter/application/pdf/vollzugshilfe_stoerfall_vo.pdf
(This guide to implementing the Ordinance on Major Incidents is also applicable to companies which are not directly subject to the Ordinance)

Bundesministerium für Wirtschaft und Arbeit, Geheimschutzhandbuch – Handbuch für den Geheimschutz in der Wirtschaft, 2005
https://www.bmwa-sicherheitsforum.de/geheimschutz/ghb.php

Bundesministerium für Wirtschaft und Arbeit, Leitfaden zum vorbeugenden personellen Sabotageschutz im nichtöffentlichen Bereich, Stand: 14.01.2005

https://www.bmwa-sicherheitsforum.de/shb/ghb/archiv/leitfaden_14.01.05.pdf

Bundesverband deutscher Banken, Management von Kritischen Infrastrukturen, 2004
http://www.bankenverband.de/pic/artikelpic/052004/br0405_rb_infrastruktur.pdf

Casavant, David, Emergency Preparedness for facilities. A Guide to Safety Planning and Business Continuity, Maryland, USA 2003

Deloitte, Erfolg in der Secure Economy – Wachstum und Wohlstand in einer sicheren Wirtschaft. Executive Summary, 2004
http://www.deloitte.com/dtt/cda/doc/content/de_public_Secure_Economy_1204.pdf

Ehses, Herbert u.a. (Hrsg.), Unternehmensschutz. Praxishandbuch Werksicherheit, Loseblattausgabe, Stuttgart, Stand: Mai 2004

Störfallkommission beim Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit, Leitfaden – Maßnahmen gegen Eingriffe Unbefugter der ad hoc- Arbeitsgruppe „Eingriffe Unbefugter“, (SFK-GS-38), 23.10.2002
http://www.sfk-taa.de/berichte_reports/berichte_sfk/sfk_gs_38.pdf

Störfallkommission beim Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit, Leitfaden für die Darlegung eines Konzepts zur Verhinderung von Störfällen gem. § 8 in Verbindung mit Anhang III der Störfall-Verordnung 2000 für Betriebsbereiche, die den Grundpflichten der Störfall-Verordnung 2000 unterliegen, bearbeitet vom Arbeitskreis MANAGEMENTSYSTEME der SFK (SFK-GS-23, Revision 1), 22.05.2002
http://www.sfk-taa.de/berichte_reports/berichte_sfk/sfk_gs_23_rev1.pdf

(The tips and information from the Hazard Commission are also applicable to companies which are not directly subject to the Ordinance on Major Incidents)

2. Internet addresses

a) Authorities:

Federal Ministry of the Interior: http://www.bmi.bund.de

Federal Ministry of Economics and Labour: http://www.bmwa.bund.de

Federal Ministry of Transport, Building and Housing: http://www.bmvbw.bund.de

Federal Ministry of Health and Social Security: http://www.bmgs.bund.de

Federal Ministry of Finance: http://www.bundesfinanzministerium.de/

Federal Office for Civil Protection and Disaster Response (BBK): http://www.bbk.bund.de

Federal Criminal Police Office (BKA): http://www.bka.de

Federal Office for Information Security (BSI): http://www.bsi.bund.de

Federal Agency for Technical Relief (THW): http://www.thw.bund.de/

German Meteorological Service (DWD): http://www.dwd.de

Regulatory authority for telecommunications and postal services (RegTP) and in future also for the areas of electricity, gas and railway infrastructure: http://www.regtp.de

b) Miscellaneous:

Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (working group on security in business): http://www.asw-online.de

German Emergency Preparedness Information System – deNIS: http://www.denis.bund.de

Kompetenzzentrum GeoRisikoForschung der Münchner Rückversicherungs-Gesellschaft (competence centre for

research on geological risks):
http://www.munichre.org (*Topics und Solutions*)

Security forum: https://www.bmwa-sicherheitsforum.de/

TSM - system for verifying organisational and technical security: http://www.dvgw.de

VDEW (association of the German electricity generating and supply industry): http://www.strom.de

Association of network operators: http://www.vdn-berlin.de

Allgemeine Informationen zur Ernährungsvorsorge:
http://www.ernaehrungsvorsorge.de

Imprint	Impressum

Published by:	**Herausgeber:**
Federal Ministry of the Interior Section P II 1	Bundesministerium des Innern Referat P II 1

Alt Moabit 101 D
10559 Berlin

poststelle@bmi.bund.de

http://www.bmi.bund.de

Editorial Department:	**Redaktion:**
Federal Office for Civil Protection and Disaster Response Centre for the Protection of Critical Infrastructures	Bundesamt für Bevölkerungs-schutz und Katastrophenhilfe Zentrum Schutz Kritischer Infrastrukturen

Deutschherrenstraße 93-95
53177 Bonn

BBK-Zentrum-I@bbk.bund.de

http://www.bbk.bund.de

Federal Criminal Police Office Section KI 21	Bundeskriminalamt Referat KI 21

65173 Wiesbaden

info@bka.bund.de

http://www.bka.de